# NISTIR 7358

# Program Review for Information Security Management Assistance (PRISMA)

**Pauline Bowen**
**Richard Kissel**

# Program Review for Information Security Management Assistance (PRISMA)

**Pauline Bowen**
**Richard Kissel**

*Computer Security Division*
*Information Technology Laboratory*
*National Institute of Standards and Technology*
*Gaithersburg, MD 20899-8930*

January 2007

## Reports on Information Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has the broad mission of supporting U.S. industry, government, and academia by promoting U.S. innovation and industrial competitiveness through advancement of information technology measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL researchers have developed detailed protocols and operational standards that improve safety of their operation, and established assessment criteria and test data sets for validation of industrial products. ITL formulates metrics, tests, and tools for a wide range of subjects such as information complexity and comprehension, high confidence software, space-time coordinated mobile and wireless computing, as well as, issues of information quality, integrity, and usability. Under the Federal Information Security Management Act, ITL is directed to develop cyber security standards, guidelines, and associated methods and techniques. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non national-security-related information in federal information systems. This Interagency Report provides an overview of the NIST Program Review for Information Security Management Assistance (PRISMA) methodology.

Abstract

Several sources of guidance, policies, standards and legislative acts provide many requirements for the federal agencies when protecting entrusted information.  Various assessments, reviews, and evaluations are an outcome of these information security requirements to monitor federal agency compliance.  The manner in which these monitoring approaches are implemented may be very different, impacting agency resource constraints.  The Federal Information Security Management Act (FISMA) of 2002 charged NIST to provide technical assistance to agencies regarding compliance with the standards and guidelines developed for securing information systems, as well as information security policies, procedures, and practices.  This Interagency Report provides an overview of the NIST Program Review for Information Security Management Assistance (PRISMA) methodology.  PRISMA is a tool developed and implemented by NIST for reviewing the complex information security requirements and posture of a federal information security program.  This report is provided as a framework for instructional purposes s to assist information security personnel, internal reviewers, auditors, and agency Inspector General (IG) staff personnel in reviewing information security programs.

# Acknowledgements

This page is
intentionally
blank

# LIST OF FIGURES

# LIST OF TABLES

This page is
intentionally
blank

# 1.  Introduction

## 1.1  Purpose

This NIST Interagency Report provides an overview of the NIST Program Review for Information Security Management Assistance (PRISMA) methodology.  The PRISMA methodology is a means of employing a standardized approach to review and measure the information security posture of an information security program.  Therefore, PRISMA is normally employed by information security personnel, internal reviewers, independent parties, auditors, and Inspector General (IG) staff personnel. Possible objectives these groups may achieve with PRISMA are to:

- Identify information security program deficiencies,

- Establish a security program baseline to measure future improvement following key personnel or organizational changes,

- Validate completion of corrective actions or the "information security posture of the program",

- Provide supporting information for the FISMA scorecard and report,

- Prepare for or conduct an assessment, evaluation, or a review of an information security program.

The points above are consolidated into PRISMA's primary objectives, which are to:

- Assist agencies in improving security/protection of federal information and Information Technology (IT) systems and their interrelated components (including contractors and state and local governments acting on behalf of federal organizations);

- Help reduce disruption of critical federal operations and assets;

- Improve Federal agency critical infrastructure protection (CIP) planning and implementation efforts;

- Support the implementation of more systematic, risk-based, and cost-effective information security frameworks and strategies.

An output of PRISMA is a maturity-based scorecard focusing on nine (9) primary review Topic Areas (TAs) of information security (see, **Table 1-1**).  This output provides executive management a clear indication of the information security posture of the agency's information security program which can be used for executive decision-making.

**Table 1-1,** *Nine Topic Areas (TA) with Sample Maturity Level Review Results*

| TA | Management, Operational, and Technical Areas | Policy | Procedures | Implemented | Tested | Integrated |
|----|---------------------------------------------|--------|-----------|-------------|--------|-----------|
| 1 | Information Security Management & Culture | 0.63 | 0.60 | 0.30 | | |
| 2 | Information Security Planning | 0.20 | 0.20 | | | |
| 3 | Security Awareness, Training, and Education | | 0.65 | 0.37 | 0.31 | |
| 4 | Budget and Resources | | 0.40 | 0.20 | | |
| 5 | Life Cycle Management | | | | | |
| 6 | Certification and Accreditation | 0.80 | 0.30 | | | |
| 7 | Critical Infrastructure Protection | | 0.60 | 0.30 | | |
| 8 | Incident and Emergency Response | 0.80 | 0.50 | | | |
| 9 | Security Controls | 0.80 | 0.60 | 0.60 | | |

Each TA above consists of Subtopic Areas (STAs: not shown in Table 1-1) and each STA consists of a number of criteria.  The first eight (8) TAs focus on the <u>strategic aspects</u> of information security program

management.  The review identifies the level of maturity of the information security program and the agency's ability to comply with existing requirements in eight areas. The last TA reviews the underlined technical aspects of the overall information security program. PRISMA therefore provides a framework to assist in instructional purposes as well as to assist assessments, independent evaluations, or reviews.

## 1.2   Legislative Background

The E-Government Act (Public Law 107-347) passed by the 107th Congress, and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States.  Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), included duties and responsibilities for the Computer Security Division in Section 303, "National Institute of Standards and Technology."  PRISMA incorporates standards from the Federal Information Processing Standards (FIPS), such as FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.  It also incorporates guidance from many of the NIST Special Publications (SPs) such as NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*; existing federal directives including FISMA; and other proven techniques and recognized best practices in the area of information security.

FISMA assigned NIST the following responsibilities:

- Developing IT standards for Federal systems, to specifically include security standards and guidelines;

- Conducting research to identify information security vulnerabilities and techniques to provide cost-effective information security;

- Evaluating private-sector policies, practices, and commercially available technologies to assess potential application by agencies to strengthen information security;

- Evaluating security policies and practices developed for national security systems to assess potential application for non-national security systems.

## 1.3   PRISMA

The PRISMA methodology was successfully employed in several independent reviews of the information security maturity of various federal agency programs over the last five years.  The methodology is a proven and successful scalable process and approach to evaluating an organization's information security program.  Simply employing the methodical approaches increased the information security awareness of security staff, interviewees, and agency personnel.  On the other end of the scale, PRISMA identifies concise security program corrective actions, which, if taken, can improve the overall security program.

The structure of a PRISMA Review is based upon the Software Engineering Institute's (SEI) former Capability Maturity Model (CMM), where an organization's developmental advancement is measured by one of five maturity levels.  This approach was incorporated into the Federal CIO Council's *Federal Information Technology Security Assessment Framework* of 2000 and PRISMA, which also employ five maturity levels where the fifth maturity level represents the highest developmental level of the information security program.  The levels are listed in increasing maturity as follow:

- Maturity Level 1: Policies
- Maturity Level 2: Procedures,
- Maturity Level 3: Implementation,
- Maturity Level 4: Testing, and
- Maturity Level 5: Integration

In PRISMA's initial maturity level of development, the review determines the existence of current, documented information security 'policies' in the federal information security program. The second PRISMA maturity level reviews the existence of documented 'procedures' developed from the policies. The third PRISMA maturity level reviews the 'implementation' of the policies and procedures. PRISMA's fourth maturity level reviews the 'testing' of the implementation of the information security policies and procedures. The highest PRISMA maturity level reviews the program or agency for 'integration' of the previous four maturity levels, i.e., information security (1) policies, (2) procedures, (3) implementation, and (4) testing. A program or agency may only attain a higher maturity level after the previous maturity level is attained. For instance, if a information security program demonstrates it satisfied the TA criteria at a maturity level three (implementation) but did not satisfy the TA criteria for maturity level one (policy), then the information security program did not attain maturity level three (nor level one nor level two in this example). 'Policy' is what defines the baseline against which all subsequent activity and maturity levels must show compliance and consistency.

**Table 1-2** shows a closer view of some of the criteria of only STA 3.1. STA 3.1 is used in other examples throughout this NIST Interagency Report. All PRISMA TAs, STAs, criteria, maturity questions, and interview questions are available in a companion file located on NIST's web site - http://csrc.nist.gov/publications/nistir/index.html.

**Table 1-2,** *Closer view of STA 3.1, some of its criteria and maturity questioning flow*

| TA | Management, Operational, and Technical Areas | Policy | Procedures | Implemented | Tested | Integrated |
|---|---|---|---|---|---|---|
| 1 | Information Security Management & Culture | 0.63 | 0.60 | 0.30 | | |
| 2 | Information Security Planning | 0.20 | 0.20 | | | |
| 3 | Security Awareness, Training, and Education | (green) | 0.65 | 0.37 | 0.31 | |
| | **STA** | **Title** | | | | |
| | 3.1 | Security Awareness, Training, and Education | | | | |
| | | Criteria: | | | | |
| | 3.1 | 1. Have employees and contractors received adequate training to fulfill their security responsibilities prior to access of the system? | Policy maturity question | Procedures maturity question | Implementation maturity question | Test maturity question | Integration maturity question |
| | 3.1 | 2. Is information security training and professional development for personnel documented and monitored? | Policy maturity question | Procedures maturity question | Implementation maturity question | Test maturity question | Integration maturity question |
| | 3.1 | Etc. | | | | | |
| 4 | Budget and Resources | (green) | 0.40 | 0.20 | | |
| 5 | Life Cycle Management | | | | | |
| 6 | Certification and Accreditation | 0.80 | 0.30 | | | |
| 7 | Critical Infrastructure Protection | (green) | 0.60 | 0.30 | | |
| 8 | Incident and Emergency Response | 0.80 | 0.50 | | | |
| 9 | Security Controls | 0.80 | 0.60 | 0.60 | | |

Section 2, *PRISMA Approach Overview*, will provide more detail on the PRISMA maturity levels and scoring.

## 1.4   PRISMA Assumptions and Constraints

A PRISMA review may be bound by several constraints and assumptions. For examples, a PRISMA review:

- May be employed to support the FISMA report,

- Uses existing agency/ program information to determine the current security program status,

- Is a 'snapshot in time' and only takes into account historical data and the data available at the time that the PRISMA review takes place,

- Is subjective using a defined methodology and assumes all interview data is valid and correct,

- Is a management level review of customizable detail to achieve defined objectives or directives,

- Is based on 'limited sample material' provided to the PRISMA Review Team. As more information is received, the review becomes a better picture of the agency's information security posture,

- The review will assist in the certification and accreditation (C&A) process, but does not take the place of the C&A process since a PRISMA review is security program focused.

- Is executed by individuals knowledgeable of FISMA, NIST standards and guidance, and security programs, and

- Is a standardized process for collecting and rating information but requires analysis by PRISMA Team member(s).

## 1.5 Audience

The audience for this document includes:

- Management personnel with a role in information security at the information security program level,

- Information Security Personnel,

- Internal Reviewers,

- Independent Parties,

- Auditors, (internal and external) and

- IG Staff Personnel.

## 1.6 Document Organization

The remainder of this document is structured as follows:

- **Section 2: PRISMA Approach Overview.** Describes the mechanics of preparing for and executing a PRISMA review, assessment, or evaluation.

- **Section 3: Application of PRISMA Final Report.** Discusses areas where the PRISMA Final Report may be applied to support and improve information security.

- **Section 4: Summary.** Discusses key points of this report.

- **Appendix A: Acronyms**. Lists acronyms and abbreviations used in this document.

- **Appendix B: Sample Memorandum from CIO to PRISMA Interviewees.**

- **Appendix C: Key Personnel Contact Request List.** List of potential interviewees.

- **Appendix D: Documentation Request List.** List of documents for the PRISMA review.

- **Appendix E: Generic Agency/ Program Questions.** Provides a basic understanding of the information security program to reduce research effort by the PRISMA Team.

- **Appendix F: Document Triage Template.** List of requested documents matched with PRISMA Topic Areas.

- **Appendix G: PRISMA Report Template.** A format recommendation for the PRISMA Final Report.

- **Appendix H: FISMA to PRISMA Crosswalk.** A mapping of the FISMA reporting requirements to the PRISMA subtopic areas.

- **Appendix I: References.**

This page is
intentionally
blank

## 2.    PRISMA Approach Overview

A PRISMA review focuses on part or all of the strategic and technical aspects of an information security program.  The review identifies the level of maturity of the information security program and the agency's ability to comply with existing requirements in the following nine (9) Topic Areas (TA):

1.  Information Security Management and Culture,

2.  Information Security Planning,

3.  Security Awareness, Training, and Education,

4.  Budget and Resources,

5.  Life Cycle Management,

6.  Certification and Accreditation,

7.  Critical Infrastructure Protection,

8.  Incident and Emergency Response, and

9.  Security Controls.

The PRISMA review is based upon five levels of maturity: policy, procedures, implementation, test, and integration.  A brief description of each level is provided in **Table 2-1**.  The PRISMA Review Team assesses the maturity level for each of the review criteria.  A higher maturity level can only be attained if the previous maturity level is attained.  Therefore, if a policy is not documented for a specific criterion, none of the maturity levels are attained for that specific criterion.

**Table 2-1,** *Description of PRISMA Maturity Levels*

| Description of PRISMA Maturity Levels |
|---|
| **Maturity Level 1:  Policies** |
| • Formal, up-to-date documented policies stated as "shall" or "will" statements exist and are readily available to employees, <br> • Policies establish a continuing cycle of assessing risk and implementation and uses monitoring for program effectiveness, <br> • Policies are written to cover all major facilities and operations agency-wide or for a specific asset, <br> • Policies are approved by key affected parties, <br> • Policies delineate the information security management structure, clearly assign Information security responsibilities, and lay the foundation necessary to reliably measure progress and compliance, and <br> • Policies identify specific penalties and disciplinary actions to be used if the policy is not followed. |
| **Maturity Level 2:  Procedures** |
| • Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies, <br> • Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed, <br> • Procedures clearly define Information security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and data processing personnel, (3) management, and (4) Information security administrators, <br> • Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance, and <br> • Procedures document the implementation of and the rigor in which the control is applied. |

| Description of PRISMA Maturity Levels |
|---|

**Maturity Level 3: Implementation**

- Procedures are communicated to individuals who are required to follow them,
- Information security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training,
- Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged, and
- Initial testing is performed to ensure controls are operating as intended.

**Maturity Level 4: Test**

- Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations,
- Tests ensure that all policies, procedures, and controls are acting as intended and that they ensure the appropriate information security level,
- Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual information security incidents or through information security alerts issued by US-CERT, vendors, and other trusted sources,
- Self-assessments, a type of test that can be performed by agency staff, by contractors, or others engaged by agency management, are routinely conducted to evaluate the adequacy and effectiveness of all implementations,
- Independent audits such as those arranged by the Government Accountability Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but are not to be viewed as a substitute for evaluations initiated by agency management,
- Information gleaned from records of potential and actual Information security incidents and from security alerts, such as those issued by software vendors are considered as test results. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risk,
- Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented, and
- The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively.

**Maturity Level 5: Integration**

- Effective implementation of information security controls is second nature,
- Policies, procedures, implementations, and tests are continually reviewed and improvements are made,
- Information security in integrated into Capital Planning and Investment Control (CPIC),
- A comprehensive information security program is an integral part of the culture,
- Decision-making is based on cost, risk, and mission impact,
- The consideration of information security is pervasive in the culture,
- An active enterprise-wide information security program achieves cost-effective information security,
- Information security is an integrated practice,
- Security vulnerabilities are understood and managed,
- Threats are continually re-evaluated, and controls adapted to changing information security environment,
- Additional or more cost-effective information security alternatives are identified as the need arises,
- Costs and benefits of information security are measured as precisely as practicable, and
- Status metrics for the information security program as well as individual CPIC information security investment performance measures are established and met.

**Figure 2-1** is an overview of a process flow for a general PRISMA review. The first four (4) steps represent preparation activities, while the remaining steps provide guidance on executing an effective review at the defined scope. The PRISMA Preparation and Execution phases are detailed in following sections.
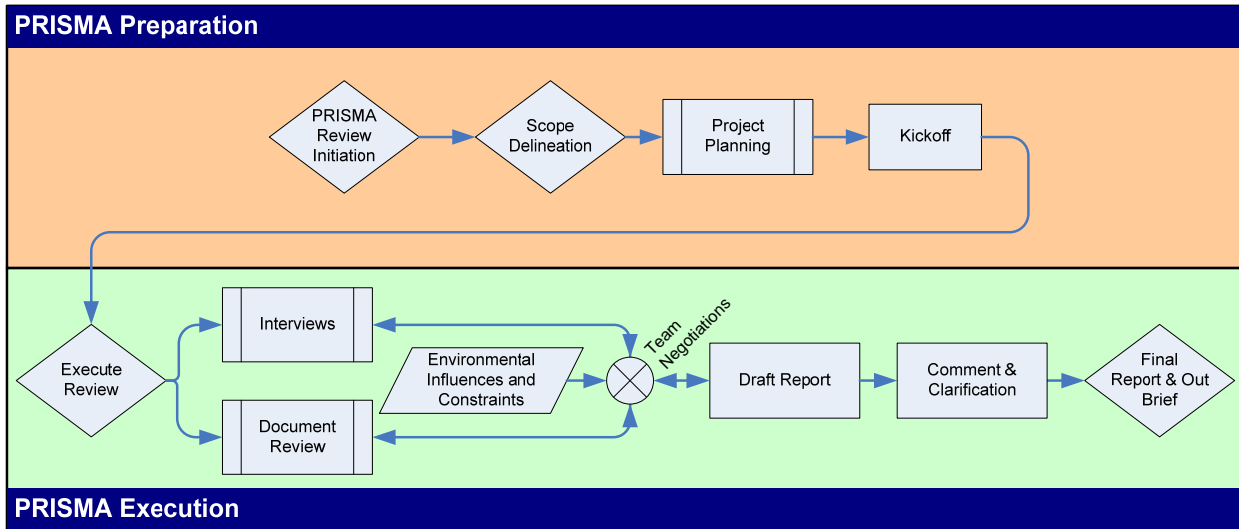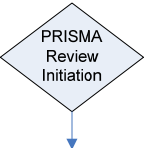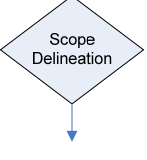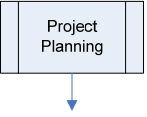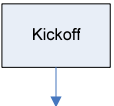


**Figure 2-1**, *PRISMA Process Overview*

## 2.1 PRISMA Preparation

This section provides a suggested approach and templates to plan and prepare a PRISMA review. The review, though, may be scaled as needed for the information security program. The approach as shown in **Figure 2-1** is the same regardless of tailoring or scaling. **Table 2-2** provides a summary of activities and outputs for the Preparation Phase.

**Table 2-2,** *PRISMA Preparation Activities*

| PRISMA Process Steps | Actions | Outputs |
|---|---|---|
| PRISMA Review Initiation | • Define management "Need" for accomplishing a PRISMA Review | • PRISMA Review Objectives<br>• Lead and supporting organizations<br>• Constraints and assumptions<br>• Appropriate Management level endorsement and authority to apply organizational resources |
| Scope Delineation | • Select Scope – Determine or demonstrate information security management capability for:<br>  o Overall Agency<br>  o Program Level<br>  o Topic Area(s)<br>  o Maturity Level | • PRISMA Review Scope Statement<br>• Project Deliverable(s) |
| Project Planning | • Resource planning<br>• Determine schedule milestones<br>• Identify roles and key personnel participants; notify key personnel<br>• Prepare/ select PRISMA criteria<br>• Identify applicable review information<br>• Tailor and respond to generic agency/ program questionnaires | • Project Plan<br>• Contract SOW, as necessary<br>• Key Personnel Contact List<br>• Memorandum to PRISMA key personnel interviewees [**Appendix B**]<br>• Document review list [**Appendix D** and **F**]<br>• Completed Generic Questionnaire [**Appendix E**] |
| Kickoff | • Present scope and objective<br>• Present schedule and PRISMA approach to Review participants<br>• Invite participation to identify additional documentation and participants | • Presentation to review team, supporting organizations, and management |

### 2.1.1 Step 1: PRISMA Review Initiation[1]

The PRISMA Review Initiation step establishes the foundation or the "need" for the review. The organizational "need" will uniquely vary with the organization and adapt to any period in time, yet may include:

- Determining the information security program gaps,

- Ascertaining program/ agency maturity levels,

- Independent validation of program/ agency information system security program, such as an assessment, evaluation, or a review, and

---

[1] In certain situations these steps may not be necessary. The policy or practice of an agency sponsor, auditor or IG team may also preclude an activity.

- An audit or inspection demanded by charter, higher authority, or other mandate.

Next, an objective or group of objectives are developed based on the "need" statement and may include:

- Identifying security program deficiencies,

- Establishing a security program baseline to measure future growth following key personnel or organizational changes,

- Justifying continued budget support for a particular information security program,

- Independent validation of the "state-of-the-program",

- Supporting information for FISMA scorecard, and

- Preparation for or conducting an IG review.

The PRISMA Review's "need" and subsequent objective statement is developed with or by the appropriate organizational management level with the authority to accomplish the review and apply the necessary resources. After capturing the "need" and codifying an objective statement for the review, the lead organization and project manager is appointed along with all supporting organizations. As a final output of this activity, appropriate management level endorsement of the PRISMA Review is crucial to the success of the review. This endorsement in the form of a memorandum or e-mail formally authorizes the PRISMA Review, captures the organizational need and objectives, and appoints the PRISMA Review leadership and team.

### 2.1.2 Step 2: PRISMA Review Scope Delineation[2]

As stated earlier, the PRISMA process evaluates the maturity and effectiveness of an information security program. The construction of the PRISMA process allows for scoping the project to support a variety of organizational needs. The PRISMA Review may be conducted for an agency or operating division security program with a focus on all nine TAs or any subset. Additionally, a review may be focused toward assessing a particular maturity level, for example, the status of the Policy maturity level.

### 2.1.3 Step 3: PRISMA Planning

This process step is primarily concerned with resource and schedule planning to execute the review and to establish the initial groundwork to prepare for the review. The initial resource question centers on whether human and capital resources exist to execute and then whether a review is conducted in-house, through contracted actions, or by an IG or review team. Another factor to consider is the appropriateness of an in-house review versus an independent agent with regards to brokering and presenting observations. If an independent, non-government agent is necessary, a primary output at this stage is a contract Statement of Work (SOW) with the appropriate PRISMA tasks and deliverables identified.

The secondary planning action is to prepare for the PRISMA Review itself by identifying primary and alternate key personnel contacts and supporting documentation based on the defined review scope. A recommended listing of key personnel interview candidates is provided in **Table 2-3**. A Memorandum from an organizationally appropriate Manager (such as the CIO) is recommended to notify and engage PRISMA interviewees. A sample Memorandum is provided in **Appendix B**.

---

[2] *ib.*

**Table 2-3,** *Key Personnel Contact Request List*

| Key Personnel Contact Request List | |
|---|---|
| Chief Information Officer (CIO) | Contract Managers |
| Chief Financial Officer (CFO) | Human Resource Managers |
| Chief Technology Officer (CTO) | Functional Area Managers |
| Senior Agency Information Security Officer (SAISO) | Program Managers |
| Inspector General (IG) Staff Personnel | Program Contracting Officers (CO) |
| Information Systems Security Managers (ISSMs)/ Officers (ISSOs) | Program Contracting Officer Technical Representative (COTR) |
| Designated Approval Authority (DAA)/ Authorizing Officials (AO) | System/ Network/ Database Administrators |
| Facilities Mgrs/ Physical Security Mgrs | IT Developers and/ or Integrators |
| Directors (IT, business areas, etc.) | End Users |

The PRISMA Review Team works with the information security program personnel to ensure the sampling of key personnel is sufficient to address the job responsibilities and organizational structure. **Appendix D** and **F** are provided to assist in identifying and collecting supporting PRISMA review documentation. **Appendix D** presents a recommended list which may be modified or shortened according to the defined scope. **Appendix F** provides a document triage matrix to match documents to PRISMA TAs and maturity levels. Documents supporting the review should be cataloged according to the title and official release date and/or draft circulation date.

During this activity, key information security or other agency representatives of the information security program under review should complete relevant questions from the Generic Questionnaire contained in **Appendix E**. Questions supporting the scope and level of the review should remain the focus; however, many of these questions are designed to provide valuable environmental and cultural support for the review.

### 2.1.4   Step 4: PRISMA Kickoff Meeting
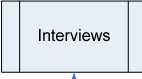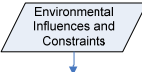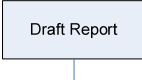
A kickoff meeting is recommended between the party implementing PRISMA (information security personnel, auditors, inspectors, etc.) and representatives of the information security program under review. At the meeting, the identified objective, scope, schedule, document criteria, and related interview approach are briefed to the participants. Secondly, the management level Memorandum may be discussed to confirm the contact information and to develop a schedule with the interviewees.

The kick-off meeting may also be used to canvas the review team (which may be information security personnel, auditors or inspectors) as well as key interview participants and organizational management for validation of and solicitation of additional information. Candidate areas for discussion include responses to the generic questionnaire, the documentation list, and additional or other interview candidates.

### 2.2   Execute PRISMA Review

The review's execution phase ultimately results in a published report and consists of reviewing agency documentation, interviewing agency personnel, and performing a review gap analysis. The PRISMA Review Team conducts the review in a fashion that minimizes the impact of the review on necessary operations. **Table 2-4** provides a summary of activities and outputs to execute a PRISMA Review.

**Table 2-4,** *PRISMA Execution Activities*

| PRISMA Process Steps | Activities | Outputs |
|---|---|---|
| Execute Review | • Initiate interviews of key personnel and supporting documentation in parallel (if practical)<br>• Track interview and document review progress metrics | • Complete weekly progress status report |
| Document Review | • Collect and catalog identified documents<br>• Evaluate documents based on the PRISMA Review scope and supporting PRISMA TA criteria<br>• Record comments and evaluation results | • Document evaluation results<br>• Supporting comments |
| Interviews | • Schedule interviews with individuals on the key personnel list<br>• Conduct interviews with key personnel utilizing tailored Interview Questions for one to 1.5 hours in length<br>• Record Interview Question responses, comments, and supporting evidence | • Responses from Interview Questions<br>• Supporting comments and information system security program evidence |
| Environmental Influences and Constraints | • Based on observation, identify environmental influences and constraints<br>• Determine underlying issues, threads, or cultural factors | • Supporting review data |
| Team Negotiations | • Periodically discuss and collaborate review results<br>• Discuss recommendation approaches | • Supporting comments and information |
| Draft Report | • Accomplish TA analysis determining observations and recommendations<br>• Complete draft PRISMA Review Report | • Draft Report [**Appendix G**]<br>  o Observations and Issues<br>  o Recommendations<br>  o Proposed POA&Ms<br>  o FISMA Gap Analysis |
| Comment & Clarification | • Submit draft Report to stakeholders for review<br>• Review comments and questions; negotiate with stakeholders accordingly | • Review comments and identified areas for clarification or update<br>• Responses to comments and clarifications |
| Final Report & Out brief | • Incorporate new observations and results from comments and negotiations<br>• Complete and distribute final PRISMA Review Report | • PRISMA Review Report |

## 2.2.1   Step 5: Document Review

Using the PRISMA Review Criteria, a member(s) of the PRISMA Review Team reviews all documents pertaining to each of the PRISMA topic areas within the scope of the review and the maturity objective of the document (i.e., a policy maturity level versus an implementation maturity level type document).  The PRISMA Review Team member(s) determines whether the document is "compliant", "partially complaint", or "not compliant" when assessed against the PRISMA document criteria.  The following is a list of items to remember when reviewing the documents:

- Policy compliance can only be found in an organizationally recognized policy document,

- Documents, especially policy and procedures must be identified as "Final" and "Approved" to be considered for maturity compliance, and

- Quantity as well as quality of documents must be considered, when necessary, in responding to certain PRISMA criteria.  In other words, if the program under review has ten applicable systems and the PRISMA Review Team receives only three fully compliant security plans for three of these systems, the PRISMA Review Team member(s) will score the results as a "partial compliance" since seven security plans are missing.

**Table 2-5** shows sample maturity level question responses based upon a document review.

Table 2-5, *Sample Documentation Review Results for All Maturity Levels of One Criterion*

| Maturity Level Question | Maturity Level Question Sample Response | Compliance Indicator | Explanation |
|---|---|---|---|
| Maturity Level 1: **Policy.** Does documented policy require controls such as separation of duties, least privilege, and individual accountability incorporated into all business operations? | Yes – *Policy Document*, Chapter 6 part 5.2 shall provide access to Organization's information systems according to individual accountability, separation of duties, and the least privilege practice. | Compliant | |
| Maturity Level 2: **Procedures.** Are procedures documented for incorporating controls such as separation of duties, least privilege, and individual accountability incorporated into all business operations? | Yes – Chapter 2 part 1.2 The Internet Posting Process provides instruction as to where, how, when, and who incorporates controls for separation of duties, least privilege, and individual accountability for posting to the Internet. This document provides a partial compliance since other functions need such procedures. | Partially Compliant | This procedure applies only to Internet posting; other events are necessary to provide complete compliance. |
| Maturity Level 3: **Implementation.** Are controls such as separation of duties, least privilege, and individual accountability incorporated into all business operations? | Yes, Section 3.3.1.1 provides general assignment of information security responsibilities based on principles of separation of duties, least privilege and individual accountability. Section 3.3.6.1 states System "X" separated users into two primary categories: superusers and users. Superusers are subdivided into 4 types: AAs, EC Reviewers, SAs, and DBAs. This document provides a partial compliance since other systems require implementation. | Partially Compliant | One system has evidence of implementing these access controls. However, this is only partial compliance for the question since this document does not provide evidence of implementation for all systems. |
| Maturity Level 4: **Test.** Are tests periodically conducted to verify that specified roles and responsibilities are separate and that a single individual does not have the capability to perform these multiple roles and responsibilities? | No, not addressed | Noncompliant | |
| Maturity Level 5: **Integration.** Is separating roles and responsibilities accepted and are standard business practices not challenged or defeated in purpose? | No, not addressed | Noncompliant | |

The document review information does not require corroboration by interviews.

### 2.2.2 Step 6: Interviews

Interviews provide information regarding information security program personnel knowledge of information in the documentation, their attitudes, etc.  For increased accuracy in measuring this information, NIST recommends that all PRISMA interviews include two review team members to ensure full documentation and understanding of all interviewee comments.  A member of the PRISMA Review Team schedules the necessary interviews based upon interviewee and interviewer schedules, attempting to schedule all required interviews shortly after the kick-off meeting.  In instances where an interview cannot be scheduled, an attempt should be made to schedule alternates as allowed while immediately bringing the situation to the attention of applicable management for resolution.

The PRISMA Review Team should ensure an adequate sampling of interviews is scheduled.  An interview session usually requires from 45 to 60 minutes depending upon the interviewee's level of involvement/ expertise in the agency's information security implementation.  The interviewers should try to conduct the interview in 45 minutes to respect the interviewee's time.  The following tips are provided for the interviewers:

- Make introductions (provide PRISMA interviewer names indicating organization or sponsor) and state the purpose of the interview

- Explain the purpose of the PRISMA Review and that the purpose of the interview is to identify strengths and weaknesses of the information security program that may not be obtainable from documentation

- Explain non-attribution of responses contained in data stores and final report.  The applicability of a non-attribution policy, though, is dependent upon the policy of the agency sponsor, auditor or inspector general.

- Do not record any name or associate interview responses with the interviewee in any way.  Again, the applicability of a non-attribution policy, though, is dependent upon the policy of the agency sponsor, auditor or IG.

- Ask only the questions assigned to the interviewee position type

- Document all responses on the interview forms associated with the question

- Ensure each answer is applicable to the question and that the interviewer understands the answer

- Ask if others should be interviewed or if the PRISMA Review Team should review associated matters

- Ask if the individual has suggestions to improve information security in the agency

- Thank the individual for their time and assistance

After the interview, both interviewers document the results of the interview independently.  The interviewers then resolve all discrepancies and produce a comprehensive interview document as soon as possible such as within two days of the interview.  The answer to each interview question must be complete, including enough information to make the question obvious.

**Table 2-6** provides various examples of interview questions and example documentation.

**Table 2-6,** *Sample Interview Question Responses*

| Interview Question | Sample Interview Response |
|---|---|
| **End User:** How and to what extent have the general rules and acceptable behaviors for the information system or IT resources you use been conveyed to you? Are you aware of the ethical use of IT resources? | Presently, as new employees join the organization they are required to take training detailing general security rules, rules of behavior, and ethical use of IT resources. This training requires verification through a test and is repeated annually. Additionally every time I log on, I am presented with a reminder of the security rules of behavior. |
| **Facility Manager:** What type of information security training (such as initial, periodic, annual, etc.) is given to facility managers to make them aware of their information security responsibilities? | As the FM, I receive the same security training as all organizational employees. No other specific training is provided. |
| **ISSO:** Is an individual assigned as an Information System Security Officer (ISSO) and are his/ her primary duties or additional duties documented? Is the ISSO trained to perform the duties of the job? | Yes, my appointment is formal and my duties are detailed in the agency's Security Manual. I received ISSO training provided by XXX and attended an industry provided training forum within the last year. |
| **ISSO:** Are information security awareness classes and briefings available for the general education and awareness of all users of the system? | Yes, all new employees are required to attend security awareness training and all employees are required to take annual refresher training. Additionally, the training division provides security items-of-interest presentations monthly on a volunteer attendance basis. |
| **General Personnel:** Is information security Awareness and Training (A&T) classes provided at least every 12 months and is attendance mandatory? | Yes, annual refresher information security awareness and training is conducted and is mandatory. |

### 2.2.3  Step 7: Environmental Influences and Constraints

Leading up to and during the PRISMA Review, the PRISMA Review Team members should identify and track positive and negative environmental influences and constraints bearing on the agency/ program information security program. Environmental influences and constraints include, but are not limited to the following:

- Budget constraints,
- Organizational mission limitations,
- Court order and governance issues,
- Organizational cultural influences, and
- Organizational structure.

### 2.2.4  Step 8: Team Negotiations

Periodically throughout the review, the PRISMA Review Team members (if the team is greater than one person) should meet to discuss progress and to collaborate review results and observations. Additionally, the team members can initiate discussions regarding review observations and recommendation approaches.

### 2.2.5  Step 9: PRISMA Analysis, Report Generation, and Review

Based on information gathered from interviews and document reviews supporting each TA, PRISMA Review Team members will subjectively determine the information security program status for each STA

as well as for the overall TA.  Additionally, the team members will identify information security issues and corrective actions, and recommend a corrective action plan[3].

## 2.2.5.1    PRISMA Data Analysis

The PRISMA Review Team's scoring process begins at the individual PRISMA criterion level where each document criterion has five maturity level questions, i.e., one question to evaluate the policy maturity level, one question for the procedure maturity level, one for the implementation level, etc.  For each criterion in a document review, the team member(s) begin at the lowest maturity level (i.e., policy) to determine compliance.  If the results to the policy maturity question for a specific criterion for all documents reviewed are "Noncompliant," the overall policy maturity level score is "Noncompliant" (see, **Table 2-7**, Criterion 1 row).  Also, all maturity levels above policy (i.e., procedures, implementation, testing, and integration) for that document criterion are considered "Noncompliant."  If the results to the policy maturity question for the specific criterion for some documents are considered "Noncompliant" but one or more document review results are "Partially Compliant," then the overall policy maturity score for that criterion is considered "Partially Compliant" (see, **Table 2-7**, Criterion 3 row).  If any of the document review results to the policy question for a specific criterion is "Compliant", but other criterion is noncompliant, then the overall policy maturity score for that criterion is considered "Partially Compliant" (see, **Table 2-7**, Criterion 2 row).  In addition, if some of the policy maturity questions of the document review results are "Partially Compliant" but when reviewed the documents cover all necessary portions of the policy maturity question, the overall result indicates "Partially Compliant" (see, **Table 2-7**, Criterion 4 row).  **Table 2-7** provides examples of how different document review responses may aggregate to four different maturity scores for four different document criteria policy questions.

Table 2-7, *Examples of Aggregation of Compliance*

| Subtopic Area Policy Questions | Document 1 | Document 2 | Policy Maturity Score |
|---|---|---|---|
| **Criterion 1 Policy Question** | Noncompliant | Noncompliant | Noncompliant |
| **Criterion 2 Policy Question** | Compliant | Noncompliant | Partially Compliant |
| **Criterion 3 Policy Question** | Noncompliant | Partially Compliant | Partially Compliant |
| **Criterion 4 Policy Question** | Partially Compliant [requirement part 1 of 2] | Partially Compliant [requirement part 2 of 2] | Partially Compliant |

The PRISMA Review Team members must be careful to ensure the review material and scores "make sense."  This may require examining documents, talking to other reviewers and interviewers, etc.  However, each criterion is a "hard requirement" where every portion of the criterion must be met to obtain credit.

If the result to a policy question for a particular document criterion is "Noncompliant," then all higher maturity levels (procedures, implementation, test, and integration) must be "Noncompliant."  If the response to the policy question for a particular document criterion is "Partially Compliant" or "Compliant", then the PRISMA Review team member proceeds to the procedure question for the same document criterion.  The PRISMA Review Team member uses the same aggregation process for the procedure, implementation, test, and integration maturity questions used to aggregate the policy maturity question result.  As soon as the result to the maturity level question is considered "Noncompliant," the remaining higher maturity levels must be "Noncompliant."

---

[3] *ib.*

Once the aggregation is completed across all document results for the TA criteria, the PRISMA Review Team member(s) must aggregate the individual criteria scores into a summary for the STA and for the overall TA. To accomplish this, the team member(s) examines all of the aggregate scores for each policy question within the STA. **Table 2-8** shows a sample of Subtopic Area (STA) criteria maturity questions and associated results by color coding "green" for "Compliant", "yellow for "Partially Compliant", and "red" for "Noncompliant". If all of the policy question results are "Noncompliant", the policy score for the STA is "Noncompliant" and all of the higher maturity level scores will also be "Noncompliant." If all of the policy maturity question results are "Compliant", the policy maturity score for the STA is "Compliant". If a mixture of any of the results occur (such as "Compliant" for one STA criterion policy maturity question and "Partially Compliant" for a different STA criterion policy maturity question), the policy score is "Partially Compliant". Each of the other maturity levels (procedures, implemented, tested, and integrated) is scored in the same way. As the PRISMA Review Team member(s) aggregate higher levels of maturity for an STA, the discovery of a "Noncompliant" maturity level causes a result of "Noncompliant" for all remaining maturity levels. **Table 2-9** demonstrates how maturity scores are aggregated for an STA. The aggregate score for the TA is generated in the same fashion from the STA scores.

**Table 2-8,** *Examples of Subtopic Area (STA) Aggregation of Compliance*

| STA 3.1 Criteria | Maturity Level Evaluation Questions | | | | |
|---|---|---|---|---|---|
| | **Policy** | **Procedures** | **Implementation** | **Test** | **Integration** |
| **Criterion 3.1.1** | Does documented policy require employees and contractors to receive adequate training to fulfill their security responsibilities prior to access of the system? | Are procedures documented for employees and contractors to receive adequate training to fulfill their security responsibilities prior to access of the system? | Have employees and contractors received adequate training to fulfill their security responsibilities prior to access of the system? | Are employees' and contractors' understanding of their information and information system security responsibilities periodically assessed? | Is information and information system security an integral part of the duties of employees and contractors? |
| **Criterion 3.1.2** | Does documented policy require information security training and professional development for personnel recorded and monitored? | Are procedures documented on information security training and professional development for personnel? | Is information security training and professional development for personnel documented and monitored? | Is the information security knowledge of personnel periodically evaluated? | Is information security training and professional development for personnel an integral part of doing business? |
| **Criteria 3.1.3 thru 3.1.4** | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| **Aggregate Scores >>>** | Compliant | Partially Compliant | Partially Compliant | Partially Compliant | Noncompliant |

**Table 2-9,** *Scorecard Representation of Table 2-8 above*

| STA 3.1 Criteria | Maturity Level Evaluation Questions | | | | |
|---|---|---|---|---|---|
| | **Policy** | **Procedures** | **Implementation** | **Test** | **Integration** |
| **Criterion 3.1.1** | Compliant | Compliant | Partially Compliant | Partially Compliant | Noncompliant |
| **Criterion 3.1.2** | Compliant | Partially Compliant | Noncompliant | Noncompliant | Noncompliant |
| **Criterion 3.1.3** | Compliant | Partially Compliant | Partially Compliant | Noncompliant | Noncompliant |
| **Criterion 3.1.4** | Compliant | Partially Compliant | Partially Compliant | Noncompliant | Noncompliant |
| **Aggregate Scores >>>** | **Compliant** | **Partially Compliant** | **Partially Compliant** | **Partially Compliant** | **Noncompliant** |

**Table 2-10** below presents the PRISMA scores of STA 3.1 aggregated in **Tables 2.9** (see, [†]Note) as well as scores for STAs 3.2 and 3.3 (see, [††]Note).  **Table 2-10** also presents the aggregated score for the entire TA 3 in the top line (see, [†††]Note).  The process for this table is identical to the aggregation process outlined in the paragraphs and tables immediately above.  **Table 2-10** is also an example of a portion of the scorecard presentation in the PRISMA Report publication.

**Table 2-10,** *Scorecard Representation of TA 3 and STA 3.1 – 3.3*

| Topic Area (TA) | Subtop Area (STA) | Management, Operational, and Technical Areas | Policy | Procedures | Implemented | Tested | Integrated | |
|---|---|---|---|---|---|---|---|---|
| **3** | | **Security Awareness, Training, and Education** | | 0.65 | 0.37 | 0.15 | | ††† |
| | 3.1 | End Users' Security Awareness and Training | | 0.75 | 0.50 | 0.31 | | † |
| | 3.2 | Security and IT Professionals with Trusted Functions Security Awareness and Training | | | 0.50 | 0.14 | | †† |
| | 3.3 | Executive and Management Security Awareness and Training | | 0.20 | 0.12 | | | |

■ = Score of 1.00
■ = Score between 0.009 and 0.999
■ = Score of 0.00

[†]Note: STA 3.1 aggregate scores
[††]Note: STA 3.2 & 3.3 aggregate scores
[†††]Note: TA 3 aggregate scores from STAs 3.1 – 3.3

Further evaluation of upper maturity levels may be completed regardless of the PRISMA scores in order to support overall program recommendations, especially if one of the PRISMA Team's objectives is to estimate the resources needed to achieve a higher maturity level.  As an example, if formal written policy and or procedures addressing a PRISMA TA do not exist (and these maturity levels are therefore non-compliant) but the TA is fully implemented, then this is a much more positive situation if the PRISMA Team objective is to achieve maturity level three (implemented).  The effort to achieve two of three required maturity levels is easier, and the overall resources need to achieve maturity level three is lower.  The estimated time to achieve the implemented level goal will also be less.

### 2.2.5.2 Issue and Corrective Action Identification

After the PRISMA Review Team members aggregate scores, the information security issues are identified. The team member(s) examine all of the scores from the document review, environmental influences and constraints, and interview information to identify the real issues affecting the information security program. These issues are the specific consequences that may realistically arise due to a lack of information security measures. The issue statement must pass the "so what" test. Examples of good issue statements are:

- "Identified system vulnerabilities may be uncorrected since no formal tracking system is in use,"

- "Information systems are endangered due to a failure to manage access rights and accounts for program managers."

Each issue statement is supported by a description of what was found that identified the issue. Along with an issue statement and description, the PRISMA Team member(s) identify recommended corrective actions the organization can employ to resolve an issue. Associated with each action is an estimate of the time and resources to implement the action.

After the PRISMA Team member(s) analyze the results for each TA, the PRISMA Review Team meets to discuss the status of each TA, the issues identified within the TA, and the conclusions reached. The review team then develops corrective actions and recommendations to improve information security.

Once all corrective actions are identified, the review team prioritizes these actions according to the corrective action's cost-benefit impact on the maturity of the agency's information security program. This prioritized list becomes the PRISMA report's action plan. The action plan is then examined to identify how many actions the organization may reasonably perform with given resource restrictions against a logical tipping point to achieve improvement in information security maturity.

### 2.2.5.3 Draft PRISMA Report Generation

**Appendix G** provides a recommended template for a PRISMA Report. The template provides suggested report organization, recommended critical content and format, and proposed supporting information.

### 2.2.5.4 PRISMA Report Review and Final Report

Appropriate management levels and stakeholders should be asked to review and comment on the draft report to validate facts and statements and to evaluate the proposed corrective actions and integrated action plan. The PRISMA Team should provide a list of requested changes and evidence to support the requested changes. The requested changes and the evidence are carefully reviewed and the PRISMA review project manager and the primary stakeholder make the final decision on changes to incorporate. The PRISMA Final Report is completed based upon acceptable changes.

# 3. Application of PRISMA Final Report

The Final Report may be applied in many ways.  For instance, the results of the report can improve the information security program's ability to identify and mitigate existing vulnerabilities, the ability to act knowledgably and wisely to protect federal IT investments, and the ability to prepare for future security threats.  During Step 1 (see, section 2.1.1, *PRISMA Review Initiation*) objectives were developed based on the "need" for the review.  The following sections will discuss possible needs and objectives where the Final Report may be applied.

## 3.1 Practical Applications of the PRISMA Final Report

PRISMA, therefore, may highlight common information security issues within the information security program.  **Table 3-1** provides examples of issues.

**Table 3-1,** *Security Issues and Impacts*

| Issues | Examples | Impact |
|---|---|---|
| Lack of formalization | <ul><li>Bob knows how to do it</li><li>Alice keeps the server secure</li><li>All of us know what must be done and we do not need to write it down</li></ul> | <ul><li>Single point of failure</li><li>Work waits until employee returns</li><li>Employee retires and new person does not know what was accomplished</li><li>Little ability to recover from disaster</li></ul> |
| Capital planning process missing information security | <ul><li>Information security not addressed as a primary component</li><li>Performance measures not included</li><li>Cost-effectiveness of information security solutions not addressed</li></ul> | <ul><li>Budgets may be cut or redirected</li><li>Adequate resources may not be applied to information security</li><li>Implemented information security solutions may not be cost-effective</li></ul> |

The Final Report therefore provides, for example, the SAISO with:

1. Recommendations from a methodical approach,

2. Overall scorecard (see, **Table 1-1**) and scorecards for each TA (see, **Table 2-10**) for easy executive management review, and

3. An estimated time to correct deficiencies based on resource impact estimates (see, **Table 3-2**).

**Table 3-2,** *Example of Final Report Estimated Time to Correct Deficiencies*
*Based on Resource Impact Estimates*

| Category | Description |
|----------|-------------|
| Short Term | Less than 6 months |
| Intermediate | 6 months to 2 years |
| Long Term | More than 2 years |

The following sections provide more examples of practical applications of the PRISMA Final Report.

### 3.1.1   Supporting Information for FISMA

A PRISMA review researches, analyzes, and provides information which directly responds to the FISMA report.  To increase the usability of PRISMA, this NIST Interagency Report provides Appendix H, *FISMA to PRISMA Crosswalk*, which maps the correlation between FISMA report questions and the PRISMA Topic Areas.  As an example, the author of the agency FISMA report may reference a current PRISMA Report for content to answer the reporting questions of FISMA.  Additionally, the PRISMA Report may stand as a supporting artifact for the agency's FISMA report.  Identifying Security Program Deficiencies.

As shown in **Appendix G**, the Final Report can identify issues, provide recommendations, and provide an estimated time to completion.  Management can then visually assess the deficiencies by Topic Areas and determine which deficiencies are the highest priorities to achieve a specific maturity level.  Management can also assess resource needs required (or deficient) to achieve the maturity goal.

### 3.1.2   Budget and Resources Justification

With the information above, the SAISO has specific material which may be incorporated into a Cost-Benefit Analysis (CBA) and tested against alternative analysis (AA).  The Final Report, then, becomes supporting material for a Capital Planning and Investment Control (CPIC) investment for the agency's Investment Review Board(s) (IRB), which is required to approve and prioritize all IT investments, including information security investments which are not integrated into other IT investments.

The Final Report recommendations based on a methodical approach, visual scorecards, and resource impact estimates can result in a strong argument for the most fundamental need of all information security corrective actions…funding and resource approval.

### 3.1.3   Information Security Awareness and Training

Information security personnel can visually see the information security program's security posture and then learn about the criteria with partial or non-compliant scores.  Correcting these deficiencies may advance the information security program to a PRISMA maturity goal or to the next maturity level.  When utilized in this manner PRISMA and the report are training tools to identify shortfalls and structure actions to improve security.

### 3.1.4   Information Security Program Benchmark

The PRISMA Report can be supported by a very granular, methodical assessment rich with information by employing the process described in **Section 2.0**.  It records dozens of information security criteria.  The PRISMA Report not only provides a general overview of the information security program, but it can also provide very important results to dozens of information security criteria in an easy to understand visual presentation—effectively a security program benchmark.  As resources and effort are applied to the

issues, management can focus on only a few or a larger portion of the deficient criteria and assess the changes and the benefits of the additional resources or efforts.  This management assessment of progress can impact future decision-making.

### 3.1.5   Independent Validation of the "Information Security Program's Security Posture"

When independent information security reviews are required, the review team may employ PRISMA as a proven and successful standardized tool set.  With PRISMA's library of criteria, an independent reviewer or evaluator may confirm the positive closure or mitigation of corrective actions.  PRISMA provides a format which can easily present the security posture of the information security program in a customizable presentation which is easily understandable by a broad range of technical and management backgrounds.  This standardized format also provides the opportunity to "overlay" previous PRISMA reviews showing not only the current state of information security, but also the information security program's maturation progress.

### 3.1.6   Review Preparation or Execution

Similar to Section 3.1.6 regarding independent validation, PRISMA provides a methodical approach to research and analyze information to determine information security deficiencies.  As members of an information security team, this information is crucial in not only being aware of the deficiencies but to develop a plan to correct or mitigate the deficiencies.  PRISMA assists in developing these strategies and actions.  This preparation can ready the information security program for an independent review.

For these same reasons, the IG team may also implement PRISMA to perform a customizable review of the information security program.  It provides a standardized platform to conduct the research and analysis to measure the information security posture of an information security program.  It also provides a format which may overlay a previous PRISMA review to evaluate the information security program's commitment to resolve deficiencies, for example.  PRISMA review reports may therefore perform as a standardized means of benchmarking and as a more consistent tool for information security programs to measure its aim at resolving or mitigating the findings of the PRISMA Review Report.

This page is
intentionally
blank

# 4.   Summary

PRISMA is a methodical and tested approach for information security personnel, internal reviews, auditors, and inspector generals to provide:

- A picture of the information security posture of the information security program for executive decision-makers and others,

- Identification of high level issues,

- Corrective actions to resolve identified issues,

- A training tool to learn what is required to advance to the next PRISMA maturity level, and

- Supporting material for funding and resource approval and priority.

PRISMA results in an improved agency capability to:

- Identify and mitigate existing vulnerabilities,

- Act knowledgeably and wisely to protect federal information systems, and

- Prepare for future security threats.

This page is
intentionally
blank

# Appendix A. Acronyms

| | |
|---|---|
| **A&T** | Awareness and Training |
| **AA** | Alternative Analysis |
| **AO** | Authorizing Official |
| **C&A** | Certification and Accreditation |
| **CBA** | Cost Benefit Analysis |
| **CFO** | Chief Financial Officer |
| **CIO** | Chief Information Officer |
| **CIP** | Critical Infrastructure Protection |
| **CMM** | Capability Maturity Model |
| **CO** | Contracting Officer |
| **COTR** | Contracting Officer's Technical Representative |
| **CPIC** | Capital Planning Investment Control |
| **CTO** | Chief Technology Officer |
| **DAA** | Designated Approval Authority |
| **FEA** | Federal Enterprise Architecture |
| **FIPS** | Federal Information Processing Standard(s) |
| **FISMA** | Federal Information Security Management Act |
| **FSO** | Field Security Office |
| **FY** | Fiscal Year |
| **GAO** | Government Accountability Office |
| **GSS** | General Support System |
| **HR** | Human Resources |
| **HSPD** | Homeland Security Presidential Directive |
| **IG** | Inspector General |
| **IRB** | Investment Review Board |
| **ISSM** | Information System Security Manager |
| **ISSO** | Information System Security Officer |
| **IT** | Information Technology |
| **ITL** | Information Technology Laboratory |
| **NIST** | National Institute of Standards and Technology |
| **OMB** | Office of Management and Budget |
| **PM** | Program Manager |
| **POA&M** | Plan of Action and Milestones |
| **POC** | Point of Contact |
| **PRISMA** | Program Review for Information Security Management Assistance |
| **SAISO** | Senior Agency Information Security Officer |
| **SDLC** | System Development Life Cycle |
| **SEI** | Software Engineering Institute |
| **SNA** | System/ Network Administrator |
| **SOW** | Statement of Work |
| **SP** | Special Publication |
| **STA** | Sub-Topic Area |
| **ST&E** | Security Test and Evaluation |
| **TA** | Topic Area |
| **US-CERT** | United States Computer Emergency Readiness Team |

This page is
intentionally
blank

## Appendix B. Sample Memorandum from CIO to PRISMA Interviewees

To: PRISMA Interviewees of [Agency] Regarding Information Security [self-assessment/ review/ evaluation]

From:

Date: August 14, 2006

The use of information technology is increasingly important for [your agency] to effectively accomplish our mission. Further, the area of information security is receiving increased scrutiny from Congress. [Your agency] is undergoing a [self-assessment/ review/ evaluation] to measure the information security posture of [the information security program].

Starting next week, [state name of PRISMA party] personnel will be at [your agency] to conduct interviews in support of that process. The first and most important reason of the [self-assessment/ review/ evaluation] is to identify shortfalls in our information security program and structure actions to improve our security. Our resulting action plan will support our efforts to plan for the future (for example, to help us justify budget and resources) and make [our agency] a safer and more secure place for all of us. With this in mind, it is of the utmost importance that we be honest and open with the [state name of PRISMA party] personnel when the interviews begin. This is the only way that [the agency] will receive a product that will be beneficial and provide the information needed to build a more secure future.

I appreciate your support on this important activity.

Regards,

This page is
intentionally
blank

## Appendix C.  Key Personnel Contact Request List

The information security program POC should provide the following key personnel contact information to the PRISMA team by the kickoff meeting.  The agency officials should indicate availability of these personnel.  Electronic copies of the information are preferred.

The PRISMA team requests identification of key personnel along with backup/ alternate personnel.  Key personnel should be identified for each agency/ organization.  Interviews last between 1 and 1½ hours.

Key personnel include:

- Chief Information Officers (CIO)
- Chief Technology Officers (CTO)
- Chief Financial Officers (CFO)
- Senior Agency Information Security Officer (SAISO)
- Inspector Generals
- Directors (IT, business areas, etc.)
- Facilities Managers/ Physical Security Managers
- Contract Managers
- Human Resource Managers
- Information Systems Security Managers (ISSMs)/ Officers (ISSOs)
- Program Manager(s)
- Program contracting officers
- Program contracting officer's technical representatives
- Other personnel designated by the SAISO or CIO
- System / Network /Database Administrators
- IT Developers and/or Integrators
- End Users

Provide the following information for each identified interviewee and backup/ alternate:

- Name
- Position title
- Organization
- Responsibilities
- Phone number
- Fax number
- E-mail address

This page is
intentionally
blank

## Appendix D.  Documentation Request List

The agency officials should provide the following documents, plans, procedures, and charts to the PRISMA team by the kickoff meeting.  This is only a recommended list which may be modified or shortened to align with the defined scope.  The agency should indicate official release date and/ or draft circulation date.  Electronic copies of the documents are preferred.

1. Policies and Procedures

    a. For personnel security
    b. For information security
    c. Information security program policy
    d. For rules and behaviors (i.e. users, network administrators, FSO, etc.)
    e. Agency specific policies and procedures
    f. Integrating into Capital Planning and Investment Control (CPIC)

2. Plans

    a. System security plans
    b. Computer security plans
    c. Enterprise-wide information security program plan
    d. Agency strategic plan
    e. Disaster recovery & contingency plans
    f. Plans of action and milestones (POA&M)

3. Documents

    a. CPIC Investment Review Board information security investment approvals for CPIC phases
    b. Solicitation documents containing information security requirements
    c. Life cycle documents relating to the review of information security controls within the life cycle
    d. Certification and accreditation documentation
    e. Risk management documentation
    f. Penetration Testing documentation
    g. Organization chart with information security roles

4. Information security training and awareness

    a. Information security training program description

5. Assessments

    a. Documents resulting from vulnerability or other assessments performed
    b. Risk assessment documentation
    c. Information security program/ agency self-assessment documentation and internal IT reviews
    d. External assessments (e.g., independent, oversight, Inspector General (IG), Government Accountability Office (GAO), etc.)

6. Lists
    a. List of General Support Systems (GSSs)
    b. List of major acquisitions/ investments

7. Agency information security relevant items specifically called out in budgets for current fiscal year and the next fiscal year

8. Information compiled or to be used as agency input to meet FISMA reporting requirements for previous or current fiscal year(s)

9. Miscellaneous
    a. Information security performance metrics/ measures (e.g., FISMA, etc.)

## Appendix E.  Generic Review Questions

The program officials should provide answers to the following questions to the PRISMA team within two weeks of the kickoff meeting.  These questions may be modified or the list may be shortened to align with the defined scope.  Electronic versions of the answers are preferred.

**Generic Questions: Answer in the context of current fiscal year appropriations**

1. How many FTE are dedicated to information security program agency-wide?  How are the FTEs spread across organizations?
2. How many individuals are working on information security for the agency?  How are the individuals spread across organizations?
3. How many dollars per organization are actually spent on information security for the agency?
4. What future budgetary and FTE requests per organization have been made for the next fiscal year for the agency?
5. Answer in the context of an agency-wide perspective on the agency's information security organization:
    a. How is the information security function implemented within your agency (e.g. centralized in a single organization, split across all organizations, centralized policy/procedure making and information security management, monitoring with decentralized implementation across the agency)?
    b. What are the various agency roles and responsibilities of the key information security organization(s) and personnel?

**Mission**

1. What is the agency mission?

**Policy**

1. What written issue-specific policy statements have been promulgated and to whom?
2. How is responsibility for implementing information security policies and procedures distributed throughout the organizations and within the agency?

**Configuration control**

1. Does the agency have a configuration control plan?
2. Does a Configuration Control Board or the equivalent direct activities in this area?

**Agency systems**

1. What interconnections exist with systems outside agency control?

**Information systems**

1. Does your agency have dependencies on information controlled by other agencies, or organizations?

**Information security awareness, training, and education**

1. Do the participating organizations have a formal information security training program?
2. Does the agency have specific information security training?
3. Does written documentation exist describing the training programs?

**Assessments and reviews**

1. Were the information security policies and procedures of the participating organization, or agency independently assessed?

**Internal reviews**

1. Were the information security policies and procedures of the participating organization, or agency reviewed internally?

**Concerns**

1. Do areas of management or political concern, of specific challenges or of changes in strategic direction exist?
2. Please describe them.

**Security incidents**

1. Describe some key previous, significant information security incidents.
2. How has the agency responded to them?

**Suggestions**

1. Where does the agency believe improvement is needed?
2. What assistance, which the PRISMA team may provide, will be most useful to the agency?

# Appendix F.  Document Triage Template

The table below assists in identifying Topic Areas (TA) covered by particular documents.  The shaded boxes identify the TAs most likely covered by the type of document in the left hand column.

*Note: This table is only an example to assist in screening the documents; actual documents may differ greatly from the suggestions in the appendix.*

**Table F-1,** *Document Triage Template*

| Document Type \ Topic Area | 1 Information security management and culture | 2 Information security planning | 3 Security awareness, training, and education | 4 Budget and resources | 5 Life cycle management | 6 Certification and accreditation | 7 Critical infrastructure protection | 8 Incident and Emergency Response | 9 Security controls |
|---|---|---|---|---|---|---|---|---|---|
| **Policies and procedures** | | | | | | | | | |
| Personnel security policies and procedures | ▓ | | | | | ▓ | | | |
| Information security policies and procedures | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ |
| Information security program policy | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ |
| Rules of behavior policies and procedures | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ |
| Agency-specific policies and procedures | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ | ▓ |
| Capital Planning and Investment Control (CPIC) policies and procedures | | ▓ | | ▓ | | ▓ | | | |

| Topic Area / Document Type | 1 Information security management and culture | 2 Information security planning | 3 Security awareness, training, and education | 4 Budget and resources | 5 Life cycle management | 6 Certification and accreditation | 7 Critical infrastructure protection | 8 Incident and Emergency Response | 9 Security controls |
|---|---|---|---|---|---|---|---|---|---|
| **Plans/** | | | | | | | | | |
| System security plans | X | X | X | X | X | X | X | X | X |
| Computer security plans | X | X | X | X | X | X | X | X | X |
| Enterprise-wide information security program plan | X | X | X | X | X | X | X | X | X |
| Agency strategic plan | X | X | X | X | | X | X | X | X |
| Disaster recovery and contingency plans | | | | | | X | X | X | |
| Plans of action and milestones | X | X | | X | | X | X | X | |
| **Documents** | | | | | | | | | |
| CPIC investment approval for each CPIC phase | X | | | X | X | X | | | |
| Solicitation documents containing information security requirements | | | | X | | | | | |
| Life cycle documents | | | | | X | | | | |
| Certification and accreditation documents | | X | | | | X | | | |
| Risk management documents | X | | | | X | X | | | X |
| Penetration testing documents | X | | | | | X | | X | X |

| Document Type / Topic Area | 1 Information security management and culture | 2 Information security planning | 3 Security awareness, training, and education | 4 Budget and resources | 5 Life cycle management | 6 Certification and accreditation | 7 Critical infrastructure protection | 8 Incident and Emergency Response | 9 Security controls |
|---|---|---|---|---|---|---|---|---|---|
| Organization chart with information security roles | X | | | | | X | | | |
| **Information security training and awareness** | | | | | | | | | |
| Information security training program description | | | X | | | X | | | |
| **Assessments** | | | | | | | | | |
| Vulnerability assessments | X | X | | | | X | | | X |
| Risk assessments | X | X | | | | X | | | X |
| Program/ agency self-assessments and internal IT reviews | X | X | X | X | X | X | X | X | X |
| External assessment | X | X | X | X | X | X | X | X | X |
| **Lists** | | | | | | | | | |
| Lists of GSSs and major acquisitions/ investments | | X | | | | | | | |
| Program/ agency information security relevant items specifically called out in budgets | | | X | X | | | | | |
| Information compiled for FISMA | X | X | X | X | X | X | X | X | X |
| Information security performance metrics/ measures | X | X | X | X | X | X | X | X | X |

This page is
intentionally
blank

## Appendix G.  PRISMA Report Template

The **Figure G-1** is an example of the structure of a PRISMA Final Report.  The items may be modified as necessary to match the scope of the assessment, review, or evaluation.  For instance, if the scope only encompasses the first three items in section 3.0 (Information Security Management and Culture; Information Security Planning; and Security Awareness, Training, and Education), all of the remaining items in section 3.0 are eliminated.
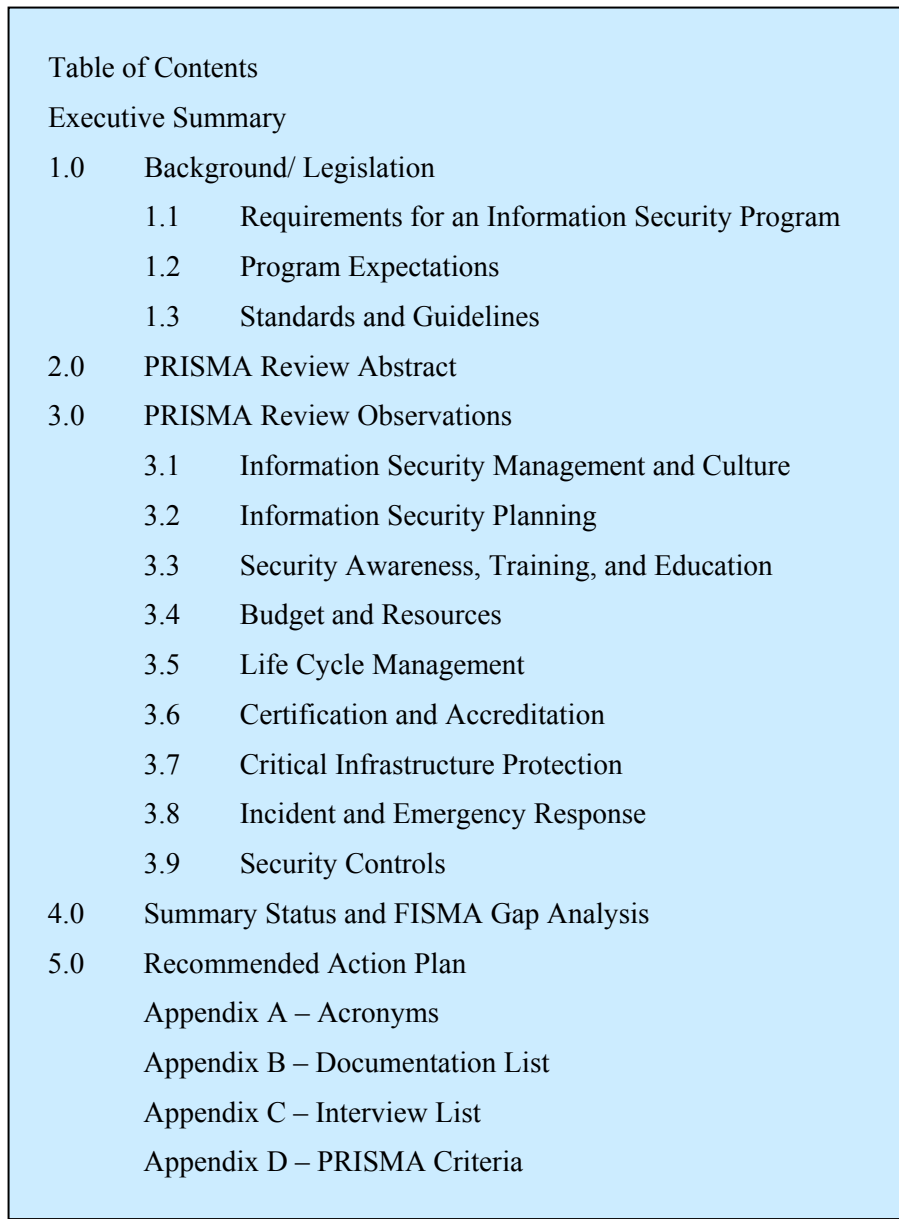
Table of Contents

Executive Summary

1.0      Background/ Legislation

       1.1      Requirements for an Information Security Program

       1.2      Program Expectations

       1.3      Standards and Guidelines

2.0      PRISMA Review Abstract

3.0      PRISMA Review Observations

       3.1      Information Security Management and Culture

       3.2      Information Security Planning

       3.3      Security Awareness, Training, and Education

       3.4      Budget and Resources

       3.5      Life Cycle Management

       3.6      Certification and Accreditation

       3.7      Critical Infrastructure Protection

       3.8      Incident and Emergency Response

       3.9      Security Controls

4.0      Summary Status and FISMA Gap Analysis

5.0      Recommended Action Plan

      Appendix A – Acronyms

      Appendix B – Documentation List

      Appendix C – Interview List

      Appendix D – PRISMA Criteria

**Figure G-1,** *PRISMA Report Template*

G.1 Executive Summary

The executive summary is the first section read and analyzed by readers, especially key management and stakeholder personnel, and therefore a very important part of the report.  The executive summary should be no more than one or two pages, summarizing all of the sections of the report.  The summary should

include key observations [positive and negative], as well as a brief summary of the proposed recommendations.

G.2 Background/ Legislation

This section summarizes the basis, or the organizational "need" and objective(s) for the PRISMA review. Additionally, it provides a background on information security and supporting legislation. Finally, individual subsections provide valuable information regarding the basic requirements for an information security program, program expectations, and supporting standards and guidelines.

G.3 PRISMA Review Activities

This section provides a brief overview of the PRISMA process, delineates the PRISMA scope for this review, and provides by reference the supporting basis for the review [documentation reviewed (see, **Appendix D**) and interviews conducted (see, **Appendix C**)]. This section provides background information for future reference regarding the review and the methodology. The PRISMA process overview may reference content from this NIST Interagency Report.

G.4 PRISMA Review Observations

This section describes the positive and negative observations within separate subsections corresponding to each PRISMA TA under the defined scope. Each subsection should provide a discussion of the salient observations discovered and analyzed from the document review and interviews. This section should capture the TA related issues and subsequent recommendation(s) in a manner which may be easily examined during post review activities. **Table G-1** provides a sample method of presenting TA issues.

**Table G-1,** *Sample Presentation of TA Issue*

| |
|---|
| **Issue 3.3-1**: The Agency's information security may be compromised due to inadequate security policy training for some employees regarding their roles and functional responsibilities. In addition, the lack of general awareness training for all employees leaves them vulnerable to common exploits such as social engineering. |
| **Recommendation 3.3-1(a)**: Complete training for all employees including executive management. |
| **Recommendation 3.3-1(b)**: Develop a comprehensive agency-wide information security training plan for all employees including new hires, employees with key security responsibilities, system users, and executive management. |

G.5 Summary Status and FISMA Gap Analysis

The Summary Status provides the overall scorecard of the TAs reviewed. It also provides separate scorecards for each individual TA and its STAs. Next, the summary provides an overall scorecard of how the maturity levels should appear for each TA after key items of the action plan are implemented. Finally, a FISMA Gap Analysis is developed from the mapping of PRISMA Subtopic Areas to FISMA requirements in **Appendix H**.

G.6 Recommended Action Plan

This section provides the recommended action plan for the information security program under the defined scope of the PRISMA Review. The recommendations should be presented in a prioritized fashion with a time frame schedule. The plan includes an accumulation of the issues and corrective actions as identified in **Table G-3**. **Table G-2** provides a legend explaining the terms and content of the PRISMA Action Plan.

**Table G-2,** *Action Plan Legend*

| Column Header | Description |
|---|---|
| **Priority** | The priority number given to a particular action. |
| **Section Area** | The corresponding subsection area in Section 4 of the PRISMA Report, where the issue is identified. |
| **Issue** | The stated issue requiring correction |
| **Recommended Action** | The corresponding recommended action for the issue. |
| **Time Frame** | The initial time period estimated to complete the initial recommended action.  If the task is recurring, an "R" will accompany the time frame estimate. <ul><li>Short Term =  Less than 6 months</li><li>Intermediate =  6 months to 2 years</li><li>Long Term =  More than 2 years</li></ul> |

**Table G-3, *Sample Action Plan***

| PRIORITY | REPORT SUB-TOPIC AREA | ISSUE | RECOMMENDATION | TIME FRAME | RESOURCE IMPACT |
|---|---|---|---|---|---|
| 1 | 3.3 | **Issues 3.3-1:** The Agency's information security may be compromised due to inadequate security policy training for some employees regarding their roles and functional responsibilities. In addition, the lack of general awareness training for all employees leaves them vulnerable to common exploits such as social engineering. | **Recommendation 3.3-1(b):** Develop a comprehensive agency-wide information security training plan for all employees including new hires, employees with key security responsibilities, system users, and executive management. | Intermediate/R | Management decision |
| 2 | 3.8 | **Issues 3.8-1:** Agency has no formal procedures for its Incident Response capability exposing the IT infrastructure and information to possible significant damage. | **Recommendation 3.8-1:** Document procedures for incident response, verify effectiveness of the procedures, and communicate them agency-wide. | Short Term | Management decision |
| 3 | 3.3 | **Issues 3.3-1:** The Agency's information security may be compromised due to inadequate security policy training for some employees regarding their roles and functional responsibilities. In addition, the lack of general awareness training for all employees leaves them vulnerable to common exploits such as social engineering. | **Recommendation 3.3-1(a):** Complete training for all employees including executive management. | Intermediate/R | Management decision |
| 4 | 3.2 | **Issues 3.2-1:** Most (63%) of the Agency's systems do not have current security plans impacting the Agency's ability to comply with FISMA requirements. | **Recommendation 3.2-1:** Establish procedures to create and update System Security Plans promptly. Enforce more accountability at PM/ Systems Owner level for maintaining System Security Plans. | Intermediate/R | Management decision |

# Appendix H.  FISMA to PRISMA Crosswalk

**Table H-1** is a mapping of the FISMA reporting requirements to the PRISMA Subtopic Areas (STA).  The PRISMA Report outlined above in **Appendix G** presents support information for the FISMA requirements intercepted at the red diamonds in this **Table H-1**.

**Table H-1,** *FISMA to PRISMA Crosswalk*

| FISMA Requirements | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 2.1 | 3.1 | 3.2 | 3.3 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 4.6 | 4.7 | 5.1 | 5.2 | 6.1 | 7.1 | 8.1 | 8.2 | 9.1 | 9.2 | 9.3 | 9.4 | 9.5 | 9.6 | 9.7 | 9.8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1  Apply standards for information categorization |  | ♦ |  |  | ♦ | ♦ |  |  |  |  |  | ♦ |  | ♦ |  |  | ♦ |  | ♦ |  |  |  | ♦ | ♦ | ♦ | ♦ | ♦ |  |  | ♦ |
| 2  Provide Protections Commensurate with risk and magnitude of harm (conduct risk assessments) |  | ♦ |  |  | ♦ | ♦ |  |  |  | ♦ | ♦ | ♦ | ♦ |  |  |  | ♦ | ♦ | ♦ | ♦ | ♦ |  |  | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ |
| 3  Establish security policies and procedures: Establish and maintain an agency-wide IT security program | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ |
| 4  Develop System Security Plans |  |  |  |  |  | ♦ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5  Develop and maintain a security training and awareness program |  |  |  |  |  |  | ♦ | ♦ | ♦ | ♦ |  |  | ♦ | ♦ |  |  |  |  | ♦ |  | ♦ |  |  |  |  |  |  |  |  |  |
| 6  Conduct annual testing and evaluation of security controls; Certify and accredit systems; Implement Continuous Monitoring |  | ♦ | ♦ | ♦ | ♦ |  |  |  |  | ♦ | ♦ |  |  | ♦ | ♦ |  |  |  | ♦ | ♦ | ♦ | ♦ |  |  |  |  |  |  |  |  |
| 7  Implement a corrective action process |  | ♦ |  |  | ♦ | ♦ |  |  |  | ♦ |  |  |  |  |  | ♦ |  |  | ♦ |  |  |  |  |  | ♦ |  |  |  |  |  |
| 8  Establish an incident reporting and sharing process: Comply with security incident reporting |  |  |  |  |  |  |  | ♦ |  | ♦ |  |  |  |  |  |  |  |  |  |  |  | ♦ |  |  | ♦ |  |  |  |  |  |
| 9  Plan for continuity of operations including information and information systems provided or managed by another agency, contractor or other source |  |  | ♦ |  |  |  |  |  | ♦ |  |  |  |  |  |  |  |  |  | ♦ |  | ♦ | ♦ |  |  |  |  |  |  |  |  |
| 10  Develop specific system configuration requirements and ensure compliance |  | ♦ |  |  | ♦ |  | ♦ | ♦ |  |  |  |  |  |  |  |  | ♦ | ♦ | ♦ |  |  |  |  |  |  |  | ♦ | ♦ | ♦ |  |
| 11  Develop and maintain an inventory of major information systems to be updated annually |  | ♦ |  |  |  |  |  |  |  | ♦ |  |  |  |  | ♦ | ♦ |  | ♦ |  | ♦ |  |  |  |  |  |  |  |  |  |  |

| | FISMA to PRISMA Crosswalk | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **PRISMA Subtopic Areas** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **FISMA Requirements** | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 2.1 | 3.1 | 3.2 | 3.3 | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 4.6 | 4.7 | 5.1 | 5.2 | 6.1 | 7.1 | 8.1 | 8.2 | 9.1 | 9.2 | 9.3 | 9.4 | 9.5 | 9.6 | 9.7 | 9.8 |
| 12 | Establish security performance measures | | ♦ | | | ♦ | | | | ♦ | ♦ | | | ♦ | ♦ | | | ♦ | ♦ | ♦ | | | | | ♦ | | | ♦ | ♦ | ♦ | ♦ |
| 13 | Integrate security requirements into the agency's capital planning and investment control process | | | | | | | | | | | ♦ | ♦ | ♦ | ♦ | ♦ | ♦ | | | | | | | | | | | | | | |
| 14 | Establish a patch management process in conjunction with configuration management procedures (Removed from FISMA Requirements, circa 2005) | | | | | | | | | | | | | | | | | ♦ | ♦ | | | | | | ♦ | | | | | | |
| 15 | Ensure security is addressed throughout the life cycle of each system. (Removed from FISMA Requirements, circa 2005) | | ♦ | | | ♦ | ♦ | | | | | | | | | ♦ | | ♦ | ♦ | ♦ | | | | | | | | | | | |
| 16 | Conduct a Privacy Impact Assessment. Update quarterly. | | | ♦ | | ♦ | ♦ | | | | | | | | | | | | ♦ | ♦ | | | | | | | | | | | |

# Appendix I.  References

Federal CIO Council, *Federal Information Technology Security Assessment Framework,* November 2000.

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004.

GAO/AIMD-12.19.6, *Federal Information System Controls Audit Manual*, January 1999.

GAO-04-394-G, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, March 2004.

Homeland Security Presidential Directive/ HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection,* December 2003.

NIST Special Publication 800-12, *An Introduction to Computer Security,* October 1995

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems,* Rev. 1, February 2006.

NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* July 2002.

NIST Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Technology Systems,* May 2004.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* September 2004.

NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems,* July 2003.

NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* August 2003.

NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.

NIST Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process,* January 2005.

NIST Special Publication 800-100, Information Security Handbook:  A Guide for Managers, November 2006.

OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, 2003.

OMB Circular A-130, *Management of Federal Information Resources*, 2000.

Public Law 100-503, *The Computer Matching and Privacy Act of 1988.*

Public Law 100-235, *Computer Security Act of 1987.*

Public Law 104-13, *Paperwork Reduction Act of 1995.*

Public Law 104-106, *Clinger-Cohen Act of 1996.*

Public Law 107-347, *Federal Information Security Management Act of 2002.*

This page is
intentionally
blank