# NIST FISMA Phase II:
# Workshop of Credentialing Program for Security Assessment Providers
# (Workshop Summary)

On April 26, 2006 the Computer Security Division hosted the FISMA (Federal Information Security Management Act) Implementation Project Phase II Workshop of Credentialing Program for Security Assessment Providers. The Workshop was held in the Red Auditorium at NIST. Over 450 attendees from federal agencies, private sector organizations and academia participated. The purpose of the workshop was to discuss requirements and possible options for the credentialing of security assessment providers. During the morning sessions attendees were provided with a detailed overview of the FISMA project, followed by the vision and strategy for FISMA Phase II, an outline of three potential credentialing options, and a preliminary set of credentialing requirements (exemplars). The participants broke into smaller groups during the afternoon session to discuss options and requirements in greater detail.

Below are highlights of participant feedback from the afternoon session by major topic area, followed by a summary of the comments received from each breakout group i.e., consumers, security assessment providers and credentialing authorities.

## Break-out Session Highlights

### A. Credentialing Program Options

In the plenary session of the Workshop, three credentialing options were presented:

- Option 1: Consumer-based Credentialing in which federal agencies draw upon established requirements to credential and acquire security assessment services.
- Option 2: Public or Private Credentialing in which public or private organizations develop and operate a credentialing process for security assessment providers based on established service provider capability requirements, evaluation criteria, and training requirements – albeit without NIST sponsorship.
- Option 3: NIST Sponsored Credentialing in which NIST sponsors (or partners with others) in the establishment of a credentialing process for security assessment providers based on established service provider capability requirements, evaluation criteria, and training requirements.

Many participants in the Consumer Breakout Session suggested that NIST explore several current models to identify possible alternatives or to ensure that the proposed credentialing program does not duplicate existing programs.

The participants in the Security Assessment Provider Breakout Session prefer Option 2 or 3 and were concerned that Option 1 was too subjective. Participants also suggested that inspectors general (IG) and contracting offices need to be involved in the development of this program

While some of the participants in the Credentialing Authority Breakout Session expressed doubt about the need for a new credentialing program, most agreed that Option 1 was insufficient and should be considered as part of a strategy that includes another option. Session participants thought that NIST needed to be involved in Option 2

## B. Individual and Organizational Competency

Several participants voiced the following concerns or suggestions about INFOSEC-related certifications:

- Current individual certifications document a minimal level of knowledge and thus do not assure that holders of those certifications can conduct certification and accreditation activities effectively.
- Individuals' specific technical expertise should be considered.
- Web-based automated certification tests should be used to reduce costs.
- Separate certification processes should be used: one for organizations and one for individuals.
- A survey should be conducted on the value of certification versus the value of experience (past performance).
- Requiring ISO 9000 or capability maturity model (CMM) compliance at Levels 3 to 5 may be good approaches for demonstrating organizational competence and maturity in the security assessment activities.
- Instead of defining training requirements, the program should define education, skills and resources capability, and training would be the methodology for acquiring that capability.

Other participants identified specific capabilities and knowledge that security assessment provider organizations and individuals should have:

- A good foundation of NIST standards and guidelines and demonstrated experience with using those documents.
- The ability to integrate specific agency requirements and internal processes into the NIST framework.
- A good management structure.

- Proficiency in a standard certification and accreditation tool set, if and when such a tool set is developed.

## C. Procurements and Proposals

Several participants expressed the following concerns:

- A standard language for expressing certification and accreditation requirements is needed.
- To ensure the success of the credentialing program, the contracting officer (CO) and contracting officer technical representative (COTR) must write the request for proposal (RFP) and the contract correctly.
- How can agencies assure that they are getting the competent individuals identified in the original response to a federal agency RFP when those individuals often are not available when contracts are awarded?
- There is much variation in technical competence within large companies.

## D. NIST Involvement

Many participants in the three break-out sessions provided guidance for future NIST activities. NIST should:

- Develop standard documents and guidelines.
- Provide templates for the security assessment plan and security assessment report.
- Arbitrate among the various credentialing program organizations.
- Design a test based on the NIST documents that another organization could administer to security assessment provider staff.
- Provide the criteria for evaluating security assessment providers.
- Provide criteria for ensuring that everyone who assesses federal agency systems does so in a common and consistent manner.
- Retain the ability to review and guide credentialing program changes and development.

# Consumer Breakout Session

The 70 government and contractor representatives who participated in this session were asked four major questions:

1. What security assessment capabilities would consumers most like to see provided by service providers and what evidence would consumers like to see for assessing confidence in those capabilities?
2. What evaluation criteria would consumers most like to see used in determining acceptable service provider proposed capability?
3. What training (areas/topics) would be most helpful to enhance:
   a. Security assessment provider competence and capability for assessing SP 800-53 security controls consistent with NIST standards and guidelines in support of FISMA? and
   b. Consumer understanding to effectively support or prepare for security assessments?
4. Of the three proposed credentialing options presented this morning, which alternative do you prefer? Why?

Breakout session participants also voiced several additional concerns (which are presented after the responses to Question 4).

## Question 1: *What security assessment capabilities would consumers most like to see provided by service providers and what evidence would consumers like to see for assessing confidence in those capabilities?*

Participants (primarily federal agency representatives) identified several capabilities that security assessment providers must demonstrate:

- Ability to perform security assessments
- Familiarity with all 17 of the security control families included in SP 800-53
- Detailed knowledge of security assessment methodologies and associated technologies
- Consistency in reporting security assessments
- Ability to document opinions in the security assessment reports
- Proficiency in the use of standard certification and accreditation tools
- Availability of a training program for all individuals supporting security assessment activities

Participants also indicated the following:

- Security assessment provider teams should have a combination of people necessary to perform a good assessment with both technical knowledge and writing skills.

- Security assessment provider organizations need to have a good management structure to be successful.
- Security assessment providers need to have a good foundation of NIST standards and guidance and demonstrated experience with using those documents. They need to understand what it takes to implement the standards and guidance. For example, how do you combine the requirements from SP 800-53A to make the assessment process efficient?
- Security assessment providers must be able to integrate agency-specific requirements and agency internal processes into the framework established by the NIST standards and guidance to effectively conduct certification and accreditation at a federal agency.
- Customers (federal agencies) must gain the knowledge that is necessary to share with security assessment providers in order for the latter to be successful in their assessment activities.

## Question 2: *What evaluation criteria would consumers most like to see used in determining acceptable service provider proposed capability?*

Participants had the following suggestions:

- Provide examples of previous work.
- Use past performance and experience; they are the best indicators of success for certification and accreditation activities
- Have a standard matrix of skills and experience so agencies can better compare security assessment providers.
- Use a (CMM) type approach to evaluate organizations so they can demonstrate increased maturity in assessment activities.
- Focus on key performance indicators; do not try to assess too many characteristics – select the key characteristics that indicate if a security assessment provider is "on-track."
- Consider separate processes or certifications for organizations and individuals.

Several participants also indicated the following:

- Evaluation criteria are one of the most helpful things that NIST can provide – not only criteria on how security assessment providers can be evaluated but also criteria to ensure that anyone who assesses federal agency systems evaluates them consistently.
- Current certifications (e.g., CISSP) document a minimal level of knowledge and, therefore, do not assure that holders of the certification can conduct certification and accreditation activities effectively.
- The quality of an organization to conduct certification and accreditation services is related to the quality of individuals. If good individuals are identified in the original response to a federal agency, those individuals are often not available when contracts are

awarded. Therefore, how can agencies ensure that they are getting individuals with comparable skills?

- The contracting officer and contracting officer technical representative must write the RFP and contract correctly to ensure the success of the program.
- GSA maintains a central contractor register database that seems to be a database of past performance by contractors. Maybe NIST could help define some questions or statistics to be used as part of this database that would help federal agencies determine the quality of security assessment providers.
- Federal agencies would like to have a test designed by NIST and based on NIST material that others could administer.

Other participants had questions like the following:

- Does this program allow federal agencies to share insight on contractors between federal agencies? Is there a way to define topics and a scale for evaluating and sharing information about security assessment providers between agencies? What are the characteristics that agencies would want to see about security assessment providers? Can NIST establish something similar to a Better Business Bureau®?
- One of the most difficult tasks for federal agencies is having standard language related to certification and accreditation activities to include in procurement documentation. Is NIST going to recommend a standard language to be included in FAR documentation?
- Does having an independent party review and evaluate security assessment providers help to establish trust between federal agencies?

## Question 3: *What training (areas/topics) would be most helpful to enhance:*

***a. Security assessment provider competence and capability for assessing SP 800-53 security controls consistent with NIST standards and guidelines in support of FISMA? and***

***b. Consumer understanding to effectively support or prepare for security assessments?***

Participants indicated that they would like to see training for individuals and for federal agencies.

## Question 4: *Of the three proposed credentialing options presented this morning, which alternative do you prefer? Why?*

Several participants indicated that there are a number of existing programs that may provide a similar evaluation of security assessment provider organizations and that these should be explored to ensure that NIST is not duplicating existing programs that are already established.

Other participants had the following concerns:

- Companies come in all sizes; large doesn't always mean good. There is too much variation within large companies. This issue must be recognized and dealt with in the program.
- How long will the credential be valid? With the number of changes to federal legislation, NIST documentation and FISMA reporting requirements, the credential would probably only be valid for 18 to 24 months.
- The FISMA Phase II program is an evolving process; knowledge must be gained and shared across agencies. NIST should retain the ability to review and guide program changes and developments.
- Different agencies provided examples of how security assessments are done in their organizations, which may provide insight into implementing an effective program at other agencies:
    - The Department of Justice (DOJ) selects a pool of contractors to conduct certification activities but, prior to beginning any of those activities; individuals who work for the contractor organizations must complete a DOJ training course and pass a test. During their first couple of certification projects, they are observed and evaluated – and any initial problems or concerns are addressed and corrected. Recertification is required every two years. Groups of contractors are managed by a team leader. This produces a team of highly competent people that knows both the NIST standards and guidance and agency-specific processes, templates, and standards.
    - For Department of Defense (DoD) NIPRNet Compliance Visits, DoD first established a standard process to conduct compliance visits then hired technically competent people to conduct the visits following the established process.

## Additional Concerns

Participants identified the following additional concerns:

- Some participants were concerned about being required to participate in the program: "I don't want to give my work to *only* a credentialed provider."
- Federal agencies need to know what auditors will require across agencies. Currently there is no consistency in how they evaluate security from one agency to the next.
- NIST must recognize the impact the IG has on day-to-day information security program issues, including certification and accreditation, at federal agencies.
- The line of business activities are beginning to look at certification and accreditation tool sets. If a standard tool or set of tools is selected, security assessment providers should be proficient in the use of those tools.
- Current tools to do not provide any added value; the tasks they perform can easily be done by hand.

- Many agencies are reluctant to connect to other agencies and are concerned that they may be accepting too much risk. Trust is required between agencies – how can this program help with this issue? Service level agreements (SLAs) should play a role in establishing this trust.
- Organizations conducting security assessments all produce a different security assessment report. Can NIST provide a standard template? It would help federal agencies to compare the reports from different security assessment providers.
- SP 800-53A can be used for all agency assessments, not just for certification and accreditation but also for FISMA assessments, continuous monitoring, etc.

# Security Assessment Provider Breakout Session

The 170 government and contractor representatives who participated in this session were asked four major questions:

1. What security assessment capability requirements would security assessment providers find: (i) most useful, (ii) obtainable, and (iii) cost-efficient to provide effective assessment services and to demonstrate their compliance to those security assessment capability requirements?
2. What evaluation criteria would security assessment providers most like to see used to determine acceptable security assessment provider proposed capability?
3. What training (areas/topics) would be most helpful to enhance:
    a. Security assessment provider competence and capability for assessing SP 800-53 security controls consistent with NIST standards and guidelines in support of FISMA? and
    b. Consumer understanding to effectively support or prepare for security assessments?
4. Of the three proposed credentialing options presented this morning, which alternative do you prefer? Why?

Breakout session participants also voiced several additional concerns (which are presented after the responses to Question 4).

## Question 1: *What security assessment capability requirements would service providers find: (i) most useful, (ii) obtainable, and (iii) cost-efficient to provide effective assessment services and to demonstrate their compliance to those security assessment capability requirements?*

Participants raised the following concerns and recommendations for the security assessment capability requirements:

- Require candidate security assessment providers to submit the certification and accreditation documents for their own internal systems as evidence of their capabilities.
- Develop requirements that are independent of the size of the company. Consider working with the Small Business Administration for feedback. Small companies could also consider partnering with each other.
- Consider different requirements for low-, moderate-, and high-impact systems.
- Consider the costs to the security assessment providers who will bear the cost burden to meet these requirements.
- Recognize there is a tradeoff between the value of producing documentation to meet requirements and the cost of developing those documents.

- Require a firewall between the staff who provide consulting services and the staff who provide security assessment services to preclude bias or conflict of interest in security assessments.
- Consider incorporating results from Common Criteria (IS 15408) evaluations that might be useful within a security assessment.
- Consider using existing organizational credentialing programs. Some of the requirements look very much like Total Quality Management (TQM) organizational requirements; CMM is similar. If an organization already meets these requirements, it should be able to capitalize on that instead of meeting the same or similar requirements for a different program.
- Need rewards for assessment providers (i.e., give credit for already demonstrated capability) and a process for verifying it.

## Question 2: *What evaluation criteria would security assessment providers most like to see used to determine an acceptable security assessment provider proposed capability?*

Participants had the following suggestions:

- The security assessment provider's understanding of the NIST documents and the system technologies (e.g., operating systems) need to be validated.
- Security assessment providers also must be able to demonstrate that they follow NIST methodology.

Several participants also indicted the following concerns:

- It may not be possible to accurately measure an individual's technical capability. It's not always possible to know the skill set that's needed until the security assessment has started.
- Consider using NSA's INFOSEC Assessment Methodology (IAM) or INFOSEC Evaluation Methodology (IEM) certifications – or the ISC$^2$'s Certification and Accreditation Professional (CAP) certification. ANSI's 17799 credentialing program should also be examined. It would be nice to get credit for certifications already obtained.

## Question 3: *What training (areas/topics) would be most helpful to enhance:*

*a. Security Assessment Provider competence and capability for assessing SP 800-53 security controls consistent with NIST standards and guidelines in support of FISMA? and*

*b. Consumer understanding to effectively support or prepare for security assessments?*

Participants voiced the following about training:

- Gaining experience takes time to develop. Training can help fill the gap.

- Web-based training would be more streamlined, automated, and not as expensive as classroom training.
- NIST may develop the training requirements but need not be involved in providing the actual training.
- Training should be cost-effective. An organization may not be able to afford to send every person to a four-day training session. What is the cost model? What are the training costs?
- The CMM – Integration (CMMI) costs between $40K and $80K, which is a tremendous burden. Add to that the overlap of multiple individuals with multiple certifications.
- The people who develop the system accreditation and self-assessment documentation also need to be trained.

### Question 4: *Of the three proposed credentialing options presented this morning, which alternative do you prefer? Why?*

Participants contributed the following opinions:

- Option 2 or 3 is better because Option 1 could allow a contract to be awarded on a subjective basis regardless of what is in the RFP.
- One business model has been overlooked – where the government assesses and credentials other government groups (e.g., GSA's FEDSIM) or the CIO organization of a large agency assesses other large entities within the same agency as long as independence is maintained.
- This matter involves the IGs and the contracting officers. They need to be onboard for the program to work.
- The NIST National Voluntary Laboratory Accreditation Program (NVLAP) can offer a great deal to this program. The Common Criteria and FIPS 140 laboratories are small businesses and they meet the respective accreditation requirements. There is concern that this credentialing program will be something different and that security assessment providers will have to pay for meeting different sets of requirements if each agency were to develop its own set of requirements.

## Additional Concerns

Participants had the following additional concerns about the program:

- Many agencies are not identifying and categorizing their systems or no one is reviewing their categorization. If these activities are not happening consistently throughout the federal agencies, it is the IG's responsibility to ensure that these activities are performed.
- IGs need criteria for how they are auditing the agencies. There is no standardized framework for how they are assessing the agencies.

# Credentialing Authorities Breakout Session

The 25 public and private sector representatives who participated in this session were asked two major questions:

1. What FISMA Phase II program-specific requirements would credentialing authorities find most helpful to develop, operate and maintain a program for assuring service provider competence and proficiency for assessing federal agency security controls in accordance with NIST standards and guidelines in support of FISMA?
2. Of the three proposed credentialing process options presented, which option do you prefer to implement this program? Why?

## Question 1: *What FISMA Phase II program-specific requirements would credentialing authorities find most helpful to develop, operate and maintain a program for assuring service provider competence and proficiency for assessing federal agency security controls in accordance with NIST standards and guidelines in support of FISMA?*

Participants had the following suggestions:

- A strategic vision statement is needed to include health and financial private sectors.
- The program should allow small, big, and non-profit organizations to participate.
- The model selected should be scalable.
- The program should provide a "seal of approval" to validate the security assessment provider.
- The program will need a process to handle complaints.
- There should be several levels of credential authorities (e.g., low, medium, and high) and a set of procedures for each level.
- The program should have three tiers: registrar, credential authority, and security assessment provider.
- There needs to be an authoritative list of credential authorities and security assessment providers.
- The authoritative list should have a "duration timeframe."
- A registrar should manage a list of credentialing authorities and security assessment providers. Some participants thought that GSA or OMB should be the registrar and that a security line of business should be included in the GSA Schedule. Other participants thought that the registrar should be reporting to a federal agency.
- NIST should serve as arbitrator.
- Standards and guidance should be developed to address assessment plans, conflicts of interest, complaints, and conflict resolution.

- The credential organization should be trained and the credential organization should train security assessment providers; alternatively, training should be provided to trainers who then instruct the trainer concepts. The notion of "training the trainers".
- Complaints about security assessment providers should be reported to the registrar and not to the credential authorities.
- The credential authority should be protected from litigation.

The participants identified several issues that need to be addressed:

- The cost of the program
- The extent of government oversight required
- The funding process for the registrar
- Limitations on the registrar and the credential authorities
- The need for more standards
- Government oversight
- Conflict resolution regarding credentialing
- Reporting complaints and issues to the registrar
- Safe Harbor litigation (Private Securities Litigation Reform Act of 1995)

Several participants thought that NIST needs to develop, provide, or consider the following:

- A standard process (for three-year periods) to maintain credentials
- Requirements to monitor the credentials
- Separation of duties for the credential authority
- Triggers/criteria for re-credentialing a security assessment provider– e.g., personnel change, acquisition of the organization

## Question 2: *Of the three proposed credentialing process options presented, which option do you prefer to implement this program? Why?*

While some of the session participants expressed doubt about the need for a new credentialing program, most agreed that Option 1 was insufficient and should be considered as part of a strategy that includes another option.

Participants had several concerns about Option 2:

- NIST involvement is needed.
- NIST should continue to develop standards and guidelines.
- More funding is needed.
- Maintaining standards is needed
- Conflict resolution support is needed.
- A registrar authority is needed.

# Conclusion

The Workshop provided very valuable feedback with some workshop attendees suggesting variations to the credentialing options presented. Additional feedback from participants will be received during the public review and comment period on draft documents scheduled for release in July 2006. A follow on workshop is planned for Fall 2006.