NIST Integrating Security into IT Capital Planning Workshop

Presentation Notes

6.4.2003 and 6.30.2003

On June 4, 2003, and June 30, 2003, the National Institute of Standards and Technology (NIST) held two workshops on Integrating Security into Information Technology (IT) Capital Planning and Investment Control (CPIC) Process. The workshop had two primary purposes:

- To present fiscal year (FY) 2003 Federal Information Security Management Act (FISMA) reporting, Plan of Action and Milestones (POA&M) tracking and reporting, budgeting for IT security, and E-government scorecard requirements
- To assist Federal personnel with translating security activities into CPIC requirements and facilitate more efficient and effective development of Office of Management and Budget (OMB) Exhibit 300 and Exhibit 53 security sections.

Over 200 Federal government employees and contractors attended the two workshops.

This document captures the proceedings of the workshops, including a summary of the modules, a listing of the questions posed by the participants, and the panel-provided answers. Workshop materials and the feedback obtained through the question-and-answer period will be used to develop an upcoming NIST Special Publication on integrating IT security into the CPIC process, which will be available for public review in late Fall 2003.

Joan Hash and Richard Kissel of NIST introduced the workshops, indicating that NIST, along with input from its partners at OMB, developed the workshop based on the "real-world" environment of each Federal agency's operations. Specifically, Ms. Hash stressed the fact that agencies currently do not have enough resources to address every security concern and indicated that prioritization is essential for effective capital planning. Following their opening remarks, Ms. Hash and Mr. Kissel introduced the team of workshop developers, organizers, presenters, and facilitators:

Presenter	Agency/Firm	Workshops Attended	Subject Area
Joan Hash	NIST	6.4.03	Introduction
Richard Kissel	NIST	6.30.03	Introduction
Kamela White	OMB	6.4.03	FISMA Reporting Instructions/Plans of Action and Milestones Guidance
Nadya Bartol	Booz Allen Hamilton	6.4.03 and 6.30.03	Requirements Overview/Breakout Group Facilitator
Holly Rollins	Booz Allen Hamilton	6.4.03 and 6.30.03	Development of the budget submission from a security point of view/Breakout Group Facilitator
John Abeles	System 1	6.4.03 and 6.30.03	Security-related CPIC roles and responsibilities/ Implementation Issues/Breakout Group Facilitator
Steve Batdorff	System 1	6.4.03 and 6.30.03	Breakout Practical Leader
Will Robinson	Booz Allen Hamilton	6.4.03 and 6.30.03	Breakout Group Facilitator
Marianne Swanson	NIST	6.4.03	Breakout Group Facilitator

Presenter	Agency/Firm	Workshops Attended	Subject Area
Elaine Frye	NIST	6.4.03	Workshop organizer
Pauline Bowman	NIST	6.4.03	Breakout Group Facilitator
Alexis Feringa	Booz Allen Hamilton	6.4.03	Breakout Group Facilitator

The workshop was designed in four modules:

- FY03 FISMA Reporting Instructions and POA&M guidance
- Requirements Overview
- Security Investment Life-Cycle Plannin g
- Breakout Session

The FY03 FISMA Reporting Instructions and POA&M guidance module was developed and presented by Kamela White of OMB. The remaining modules were created and presented by the NIST-led team of experts to address the following key learning objectives:

- Identify relevant OMB and other guidance that applies to Federal Government IT security investment decisions
- Comprehend how current security requirements relate and support the IT CPIC process
- Understand the CPIC process phases: select, control, evaluate
- Identify CPIC-related roles and responsibilities
- Examine best practices IT security management processes and why they are important for making sound IT security investment decisions
- Understand how to develop security requirements and appropriate supporting documentation for IT acquisitions
- Identify steps and materials required to complete sound business cases in support of investment requests
- Understand implementation issues associated with incorporating IT security into the CPIC process.

FISMA Reporting Instructions/Plans of Action and Milestones and OMB Capital Planning Guidance – Kamela White (OMB) – 6.4.03

Kamela White of OMB addressed the workshop participants, focusing her remarks in four areas:

1. FY03 FISMA reporting
2. Remediation (POA&Ms)
3. Budgeting for IT security
4. Electronic Government (e-government) scorecard

FY03 FISMA Reporting

While the FY03 FISMA reporting guidance had not been officially released at the time of the workshop, Ms. White offered insights into what Federal personnel could expect from the forthcoming guidance. Her remarks appear below.

- FISMA legislation is remarkably similar to GISRA; therefore, not many changes in reporting will be required.
- The most noticeable change in the legislation is a change in NIST's role regarding issuance of guidance to agencies.
- FY03 reporting guidance will be similar to FY02 GISRA reporting guidance; specific IT security reporting requirements do not contain any drastic differences.
  - There will be no substantive changes.
  - There will be no open-ended questions.
  - All questions will focus on specific milestones and performance measures.
  - Minimal narrative will be required.
  - One noteworthy change to expect will be for agency Offices of Inspector General (IG) to review whether or not the agency has a robust POA&M process in place department-wide.
    - OMB is looking for consistency across departments so all operating units are reporting in a similar way and with similar granularity.
    - OMB's role is not to independently review all POA&Ms; rather to ensure there is a Department-wide process in place.
    - As weaknesses are identified, they need to be included in the POA&M process along with resources necessary to fix the weaknesses, the names of the individuals responsible, and milestones that all information can be tracked.
- FISMA guidance will include formatting changes; specific tables will be provided for responses to questions to standardize reporting.
- The FY02 GISRA report was just issued to Congress by OMB; while security compliance numbers were low across the board, definite progress against performance measures reported in FY01 was observed.

Following her remarks on FISMA reporting, Ms. White took questions from the workshop participants. Their questions and her responses appear below.

- FISMA changed the process of GISRA from both IG and agencies reporting to OMB and OMB reporting to Congress to IGs reporting to OMB and agencies reporting directly to congressional committees. What is the preferred process?
  - The OMB preference is to receive one report from each agency. However, an agency IG may choose to provide a separate report for a specific reason.
  - OMB will request that agencies submit reports to OMB for review (identify, fix, and avoid errors) before submitting them to Congress.
  - Agencies are still ultimately responsible for submitting reports to Congress, but OMB would prefer to review them before final submission. This process will be spelled out in the forthcoming guidance.
- What is the current estimate on when OMB will publish the FY03 FISMA guidance? Agencies are concerned because the FISMA reports are due to their internal reviewers in about six weeks.
  - OMB will release the guidance as soon as possible. Guidance is currently being reviewed by the OMB General Council and will be released after this review is complete and the new OMB Director signs the guidance.
  - Until the new guidance is released, agencies should use the FY02 guidance because the same data will be required for reporting in FY03 as was required in FY02.
- Some agencies have many weaknesses identified in POA&Ms, while some have only a few weaknesses identified in POA&Ms. If one follows the guidance, one could identify thousands of weaknesses. What is the right level of detail? High, low, etc., what is appropriate?
  - The guidance is purposefully too vague to allow for flexibility among agencies. The agencies will recognize weaknesses that they see regularly. OMB presupposes that agencies will make a judgment call on the appropriateness of weaknesses in the POA&Ms; in other words, if it takes longer to put a weakness in the POA&M than to fix it, it should be fixed and not included in the POA&M. While this is an extreme example, it conveys the point that agencies need to make a judgment call regarding the appropriate level of detail for their POA&Ms.
  - Some agencies only report materials weaknesses. OMB does not find this practice acceptable. POA&Ms should contain all types of weaknesses. OMB will consider including additional specific examples in future guidance.
  - POA&Ms are tools for agencies to track weaknesses and remediation actions—not just a reporting requirement; therefore, OMB would like to continue to receive feedback from the agencies on what appropriate reporting/levels of guidance are/should be.
- What does a “robust POA&M” mean?
  - This topic is discussed in the FY02 POA&M guidance
  - Agencies should ensure that all work is not occurring solely within in the Office of the Chief Information Officer (OCIO).
  - Program leads need to be responsible for making sure systems are secure.
- Many systems are managed at the enterprise or interagency level; this puts the burden on the OCIO. How is responsibility for such systems assigned? To a program official or CIO?
  - In this case, the CIO is truly the system owner; therefore the CIO has the responsibility of a program official and is responsible for POA&M for these systems

  - In some cases, the CIO is the owner, but another security officer is really responsible for security on the system. In such a case, the security official needs to be accountable.
  - If ownership is assigned to a board, list board in the POA&M, including individual names to increase accountability.

- The Critical Infrastructure Assurance Office (CIAO) has changed its methodology for Project Matrix from an asset approach to a critical function and services approach. However, the CIAO is not following such a scheme for data call purposes. Therefore, what is OMB expecting from agencies for Project Matrix, especially when they cannot contact/obtain necessary information from the CIAO?
  - OMB will not hold agencies responsible if they cannot contact CIAO, but agencies need to identify critical assets, regardless of whether they are successful in contacting CIAO.
  - Agencies are responsible for identifying and securing their critical assets regardless of the methodology used.

- POA&Ms are part of an overall security program and have to tie specifically to Exhibit 53 and Exhibit 300. However, this is impossible in some agencies. Is OMB asking agencies to tie POA&M items specifically to Exhibit 53s and Exhibit 300s?
  - Every agency submits an Exhibit 53 and Exhibit 300. FY01 guidance states that IT investments with POA&Ms need to tie to Exhibit 300s.
  - The Exhibit 300 is a business case/justification; some of the costs listed in Exhibit 300 may include increased security costs because of identified weaknesses.
  - The POA&M is a justification for security funding identified in the Exhibit 300. Therefore, it just needs to be referenced in the Exhibit 300.This relationship is spelled out further in FY05 guidance.
  - The POA&M is a living document. Just because a weakness has been mitigated, it does not necessarily mean that your security funding is going to get cut.

- Are 300s and POA&Ms supposed to balance? In other words, should the POA&M dollar amount match the Exhibit 300 security funding request?
  - No because POA&Ms are a subset of security funding; agencies will always have ongoing costs that are not included in POA&Ms.
  - The POA&M and Exhibit 300 totals will not be equal.
  - The unique ID number on 300 and POA&M will match. That is the link between the two documents.

- How does the POA&M reflect improvements made to system; i.e., hired full-time equivalents, purchased software, etc., to mitigate risk? After the POA&M is closed, how do you justify continuing (O&M) funding?
  - Once a weakness in the POA&M is closed, agencies will still receive justified security funding.
  - The Exhibit 300 contains sections for ongoing costs (O&M). This total does not have to balance with POA&M dollar amounts.

- OMB guidance for Exhibits 53 and 300 stresses consolidating business cases from stovepipes, but investments have to be maintained as steady state. Therefore, how do you define security funding without double counting for consolidated investments?
  - The answer to this question depends on where the agency is in its consolidation.
  - If the agency is still maintaining separate systems, they need to be defined in separate Exhibit 300s.
  - If systems are fully consolidated, the agency can bring them together under one infrastructure Exhibit 300.
  - The latest release of OMB Circular A-11, which is available on the OMB website, explains this scenario.
  - OMB will look at Exhibit 300s early if agencies would like feedback. Agencies need to submit Exhibit 300s during the summer for feedback.

Remediation

In addition to her POA&M comments above, Ms. White offered the following specific comments about remediation:

- Quarterly POA&M updates to OMB are part of quarterly assessment of agency status under the President's Management Agenda (PMA).
- These updates are still required under FISMA.
- In addition, agencies should report FISMA IT performance measures quarterly.

IT Security and Capital Planning

Ms. White offered the following comments on IT security and capital planning:

- The FY04 A-11 guidance contains a security and privacy section with straightforward questions requiring yes/no responses with relevant dates.
- OMB discovered a huge number of legacy systems with either no certification and accreditation (C&A) or an outdated C&A. GISRA reporting indicates progress, but more progress is required, especially because some of those systems are mission critical.
- As a result, OMB classified a high number of IT investments as "at risk" in FY02. Of the $59 billion IT budget across the government (of which $4.9B was for IT security for the 24 large agencies), $20B were funding investments that were at risk, and $19B were solely or in part because of IT security weaknesses.
- OMB is working with agencies to identify resources to fund mission critical systems' security, including efforts to redirect funding from lower priority investments. Agencies can also find funding on their own.
- Since the same A-11 questions will be required in FY05, this will continue to be an issue. A "no" response to security questions for an operational system will automatically place the system "at risk."
- Agencies are strongly advised to include future C&A dates in Exhibit 300s to indicate that planning has taken place.

- A-11 provides guidance on security areas for determining security costs in Exhibit 300. Estimates are required in Exhibit 300. Without responses, systems will be considered “at risk.”
- When assessing system security, OMB evaluates the Exhibit 300 depending on whether or not the system is new or operational. New investments are not necessarily expected to have C&A or plans.

Following her remarks on IT security and capital planning, Ms. White took questions from the workshop participants. Their questions and her responses appear below.

- Is there a low-high range for percentages of total funding for system security planning?
  - Depending on the system, ranges are from 1% to 17% of the total investment.
  - NIST is looking into minimum standards for systems and will provide benchmarks in the future.
  - Ten percent is a common percentage of total funding found on agency Exhibit 53s, but this percentage will vary depending on systems/agency/etc.
- As a follow-up comment, the Federal Government is averaging 8% for security on IT budget according to Gartner research.
  - There is a large variance from large to small agencies. Usually 4 to 8% overall for security as a percentage of IT budget is common.
- On Exhibit 300s, there are several questions on “how does the agency accomplish *X*,” or “how does the agency accomplish *y*” (i.e., how does the agency ensure privacy?). Should the same response appear in all Exhibit 300s to standardize agency responses? What does OMB want to see?
  - The OMB Exhibit 300 guidance has more specific information for each question, but OMB wants, in general, to see how the specific system is secured.
  - The privacy section will be handled slightly differently. Ms. White did not address privacy requirements and recommended following up with Eva Kleederman, an OMB privacy expert.
  - While security and privacy are grouped together, they are not scored the same way
  - The big issue on privacy is that new investments must perform Privacy Impact Assessment (PIA). This is included in the FY05 A-11 guidance.
- If an agency has an existing privacy record system (legacy) and is changing/upgrading, a system of records, does the agency need to perform a PIA?
  - Yes.
- How does the Government $59B IT security budget break out across the agencies?
  - Nearly that entire figure is spent by the 24 large agencies.
- Will there be E-authentication initiative questions in Exhibit 300s?
  - No.
- The OMB website is not clear on the latest versions of various guidance. Are there any plans to update the website?

- Drafts are located on the NIST website, the CIO council website, and emailed through distribution lists: IG distribution list, interagency councils, small agency council, and others.

- If anyone would like to receive the drafts via another distribution list, forward contact information to Ms. White.

- OMB releases no more than one draft for agency comments.

- What is the definition of "major change to a system"?
  - OMB Circular A-130, Appendix III addresses the definition in a high-level discussion.

- FISMA reports are is due in September. It's now June. Until FY03 guidelines come out, it is difficult for agencies to develop responses.
  - FISMA reporting due at budget submission, which is September 9 this year.
  - No new information is required in this year's FISMA reporting guidance in relation to last year's GISRA reporting guidance. Agencies should use FY02 GISRA reporting guidance to begin developing their responses.

Wrap Up

Ms. White offered the following concluding remarks on the PMA and the E-government scorecard.

- The PMA electronic scorecard is expanding. It will assess IT security on a quarterly basis. Security is an area that can keep an agency from getting from red to yellow and from yellow to green.
- For an agency to obtain a "green" rating, the agency must meet the following three criteria:
  1. IG certification that the agency has a robust POA&M in place.
  2. Majority of IT systems meeting OMB IT performance measures criteria contained in the FY02 guidance. (90% of ALL systems must comply).
  3. Consistent progress in weakness remediation demonstrated through POA&M quarterly updates. Progress must be demonstrated quarter by quarter to prove that the agency is fixing old weaknesses and identifying new weaknesses as time progresses.

- For an agency to get a "yellow" rating, the agency must meet *two* of the following three criteria:
  1. Obtain IG approval of robust POA&M process.
  2. Demonstrate consistent progress on quarterly updates, *or*
  3. Meet performance measures criteria contained in the FY02 guidance for 80% of the agency's systems.

- Scorecards are taken very seriously by the President and OMB as a performance management exercise, and will continue to be an important scoring component.

Following her remarks on the PMA, Ms. White took questions from the workshop participants. The lone question and her responses appear below.

- Is the IG review based on OMB guidance?
  - Yes. Reviews are based on specific OMB guidance, not on other items identified by IG outside of OMB guidance.

Requirements Overview

The requirements overview section addressed the following learning objectives:

- Understanding OMB, NIST, and other guidance that applies to governing Federal Government IT security investment decisions
- Identifying relationships among current requirements for IT CPIC requirements
- Learning the steps of the CPIC process
- Understanding the basics of risk management and its importance
- Identifying the different types of investment risks in addition to security risks.

Security Investment Life -Cycle Planning

The security investment life-cycle planning section was further divided into three subsections. The subsections and their learning objectives appear below.

Security-related CPIC Roles and Responsibilities

- Learn the roles and responsibilities of agency officials regarding the integration of IT security into the IT CPIC process.

Development of Budget Submission from the Security Point of View

- Identify key milestones and activities of the IT CPIC process
- Learn best practices for prioritizing IT security corrective actions for implementation
- Gain an understanding of how to develop security requirements and appropriate supporting documentation for IT acquisitions
- Identify steps and materials required to complete a sound business case in support of investment requests.

During the workshop, the facilitator asked the participants for examples of security themes within their agencies. Examples of responses included using the OMB PART tool and getting to green on the PMA scorecard.

Implementation Issues

- Learn about the iterative nature of security integration into the CPIC process
- Identify issues of security decision-making thresholds and legacy system security funding
- Understand how security activities overlap with CPIC activities for multiple budget years throughout a single fiscal year.

Breakout Session

The breakout session provided a hands-on practical exercise that illustrated an approach to prioritizing security corrective actions in a POA&M. Groups analyzed a hypothetical government agency's POA&M and developed prioritized corrective action implementation plans to submit to the agency Investment Review Board (IRB).

Workshop Questions

The following questions were posed by workshop participants in two question and answer (Q&A) sessions. The first session was conducted immediately following the lunch break and covered general administrative questions, requirements questions, and security-related CPIC roles and responsibilities questions. The second Q&A session covered several topics, including development of the budget submission from a security point of view and implementation issues. The questions and answers provided by the workshop panel appear below.

Morning Q&A Session

- Has a message been sent for the next workshop session?
  - The next workshop will take place on Monday, June 30, at the Rockville Doubletree hotel. Information will be posted on the NIST website: csrc.nist.gov

- Are electronic copies of the presentation available?
  - Yes. Materials will be posted on the NIST website.

- Are there best practices for security performance measures, business cases, and other items discussed today posted on NIST website?
  - Yes. Draft NIST SP 800-55 contains an IT security metrics development process, an IT security metrics program implementation process, and examples of IT security metrics mapped to NIST Self-Assessment Guide, SP 800-26.
  - The guidance coming out of today's workshop will have additional examples.

- How are public key infrastructure (PKI) certificates for user authentication addressed in FISMA?
  - FISMA does not go in depth on PKI authentication issues; rather it presents broad explanations.
  - In support of E-government initiatives, NIST is in the process of updating e-authentication guidance.

- On the electronic scorecard, to get to green, 90% of systems need to have completed C&A. Does the 90% constitute just-completed systems, or completed and planned systems?
  - NIST cannot speak for OMB, but will seek clarification. It sounds like the 90% includes only completed systems.

- Risk assessments have evolved not only to identify risks, likelihood, and impact, but also to provide a comprehensive evaluation of technical and nontechnical controls. This evaluation seems redundant with C&A and a waste of time. Can risk assessments be part of the C&A process?
  - A thorough evaluation of risk can be included in C&A.

- Will NIST or OMB identify roles or functions for government personnel that should not be performed by contractors?
  - NIST will not define roles, but has published a guidance document that delineates types of services that can be used via outsourcing. (NIST SP 800-35).

– NIST cannot speak for OMB.

- What is a security metrics program and where can I find an example?
  - Draft NIST SP 800-55, to become final soon, contains this information.
  - Metrics examples in NIST SP 800-55 Appendix A correspond to 800-26 critical elements.
- Are CIOs encouraged to adopt themes through CIO council or otherwise?
  - The PMA contains the highest-level themes; OMB scores are higher for those Exhibit 300s that are linked to the PMA.
  - Following PMA themes, agency-specific themes would constitute the next highest level.
- On slides 26-27, what are select, control, and evaluate?
  - These are IT investment life-cycle terms, published several years ago by General Accounting Office (GAO) to describe the investment life cycle (for example, in GAO/AIMD-10.1.23, Information Technology Investment Management, *A framework for Assessing and Improving Process Maturity*, dated May 2000).
  - Select: analytical activities (i.e., business case) to select path forward
  - Control: once a solution has been selected and acquired, the investment is monitored for schedule, budget, and functionality returns
  - Evaluate: evaluation of particular milestones in terms of timing, budget, and other issues. Did the investment solve the business problem?
- How can you prioritize a project before a business case is completed and do you have a document that completely explains the investment?
  - Subsequent slides will address the subject of a concept paper that can be used for this purpose.
  - A concept paper describes high-level goals and objectives of the proposed investment.
  - Prioritization can begin upon acceptance of the concept paper by an agency IRB.
- About two thirds of the risk categories presented in the workshop are also security categories. Does security then become a part of risk management?
  - No, because these risks are investment risks, not security risks.
- I believe OMB should use their own tool, PART, to legitimate IT security in agencies' budgeting process.
  - NIST noted the comment and will pass it along to OMB.
- Will OMB consider all Exhibit 300s for agencies that do not meet a minimum capital budget?
  - OMB will not consider all 300s. Agencies should put forth due diligence to identify the systems that will have the greatest impact on the agency and develop 300s for those systems.
- What are the criteria for an agency to submit Exhibit 300s?
  - Criteria (cost thresholds) are specific to each agency. Your agency Investment Review Board should have guidelines.

- If your agency does not submit an Exhibit 300, how can OMB provide authorship in this area?
  - If you do not submit 300, you will not receive additional funds for discretionary projects.
- How does OMB expect you should include your personnel costs? e.g., system administrators, ISSOs, CSO, IT Security Program Management and Compliance personnel? Do these go across system 300s or the Exhibit 53?
  - Government FTEs are captured in the summary of spending table under the Government FTE row. In theory, these costs should be embedded in planning or O&M costs captured in rows above. Rules of thumb: if a position can be mapped to a given project, you should include their salaries in the Exhibit 300 for that project. If personnel are performing security functions, they should be captured in Part B under FY05 security costs.
  - Not 100% of your agency's budget is in your 300. On the exhibit 53, you can capture other costs, including cross cutting personnel costs.
- The POA&M is purely passive/historical. Point: we need to remind individuals to plan for future security costs or weaknesses that will occur (i.e., future C&A costs, etc., and for legacy systems as well).
  - The response to this statement appears below the following question.
- How does OMB evaluate your POAM if you are truly looking at the cause of your weaknesses and you plan a large automation system (i.e., policy automator) and you will need to put that into the 2-year out budget cycle?
  - Some elements of this question were addressed during Kamela White's discussion on June 4th. Please reference that synopsis contained in the workshop notes. Additionally, the prioritization approach in the workshop will help you develop a plan for implementation. Yes, the POAM is historical, but it should provide inputs into your Exhibit 300s.
  - You have to have a unified POAM process as Kamela White explained on June 4th. Look for the causes of problems rather than the symptoms.
- Is the FISMA reporting guidance currently available? If so, where?
  - No, but the guidance should be released soon.
- When will SP 800-53 be available for review?
  - NIST does not know the exact date at this time, but Richard Kissel will be available for specific questions following the workshop. The forecasted release date is August 1st.
- Is the select-control-evaluate process conducted each year for a single system/project?
  - No, you do not perform the entire process every year. Parts of process will differ each year depending on where you are in the investment lifecycle. On the front end, you do more selection and control during the lifecycle and annual milestone evaluations, and then functional evaluations at the end of the lifecycle.
- Feedback for facilitators: on page 27, media sanitization occurs in the operations and maintenance and the disposition phases.
  - The feedback was noted.
- 800-55 was mentioned several times, what is it about. How do you capture metrics.
  - NIST 800-55 is entitled "Security Metrics Guide for IT Systems." It provides a process for identifying and implementing a security metrics program. It is currently in draft format; the final will be available after the FISMA guidance is released. The planned changes between the current draft and the anticipated final are minimal.

  - The guide contains 20-30 pages of narrative, describing the creation and implementation of a mature metrics program. The remainder of the document contains metrics that align with NIST SP 800-26. Each metric has a one-page form with information on how to interpret and utilize the metrics.

- The workshop is called integrating IT security into Capital Planning. However, the terms that are used are confusing such as ROI, NPV, etc. Security is a cost activity. It does not provide any ROI unto itself. The ROI is in the overall IT investment, which supports an agency's mission. The goal for IT security is to mitigate risks while the IT investment supports the goals/missions. Therefore, IT security is identified as an element in lifecycle planning.
  - A security investment could have ROI and NPV if the investment was enabling a service that could not be performed without a specific security-related technology. Additionally, if you are considering different alternatives, some will have higher ROIs and NPVs.
  - ROI and NPV are not optional; they are required for comparing alternatives in the 300.
  - If security is buried as part of an IT investment, ROI for security will not be the overriding factor.

- True or false, 80% of major as well as non-major applications must have completed C&A by the end of FY03?
  - True

- Should there be a one-to-one correspondence between systems and applications contained on the 300 and the systems and applications that you used NIST 800-26, or can there be more NIST 800-26 systems than wheat are reported to OMB?
  - You will perform 800-26 self assessments for all systems, while you will develop Exhibit 300s for those that are above the threshold.

Afternoon Q&A Session

- Security staff should not be forced to save the day. If OMB is doing its job, why are legacy-hungry CIO pet projects still occurring?
  - CIO's are expected to define the strategy to be implemented and lead their organizations in this exercise by and objectively applying the criteria agreed upon. In many cases perceived "Pet Projects" have a high priority based on external interests, congressional interests or other information not available at lower levels in the organization. In the best scenario, projects moved forward are accompanied by well-documented justifications.

- On slide 37, what is GPEA?
  - GPEA stands for the Government Paperwork Elimination Act.

- What are presenter's names? Please put them on slides.
  - The presenters are identified in the beginning of this workshop summary.
  - Joan Hash is the point of contact for any comments.

- What is considered "high impact" as it relates to POA&M issues?
  - As an example, establishing a configuration management capability should have higher impact than fixing specific vulnerability within a single system.

  - In general, agencies should seek those corrective actions that can be implemented for lower cost, while fixing larger problems, in other words, the highest value and lowest cost. Criticality of a system is incorporated into the decision criteria.

- Are all projects prioritized only using information from concept papers?
  - No. Concept papers are outputs from prioritization process.
  - You prioritize your own POA&M corrective actions.

- Are major and minor projects prioritized together?
  - All POA&M items should be prioritized.

- What do you do if prioritization is wrong?
  - The CPIC process presents a structured approach to prioritizing corrective actions. However, agencies can adapt the process to meet their particular needs and situations. If an agency realizes throughout the course of the year that its prioritization was not effective, the prioritization criteria for the following year should be updated to reflect the lessons learned.

- Why not prioritize after the select phase?
  - Because of tight resources (in both personnel and financial resources), it is prudent to prioritize first.

- In the prioritization chart, the upper right quadrant is funded first and the lower left quadrant is funded last. How do you prioritize middle?
  - Stakeholders must debate this issue, as prioritization factors germane to the agency will need to be examined.

- If you have an investment that has been approved at the concept level and it is time to write an Exhibit 300, how many of the Exhibit 300 entries will not apply?
  - In general, all answers should be provided in a thorough concept paper.
  - From the NIST/OMB perspective, are all mission-critical systems defined as major applications (MA)?
  - No. Backbones should be identified as mission-critical general support systems (GSS)

- How do major systems referred in FISMA relate to NIST MA and GSS definitions?
  - They do not relate. MAs or GSSs can be classified as major systems.

- In the breakout session, the practical exercise demonstrated a spreadsheet tool where one column on the spreadsheet was labeled ‘Corrective Action Impact.’ What does this mean?
  - The corrective action impact is the compliance gap of a security corrective action divided by the cost to fix the compliance gap. So, if the agency finds the compliance gap (the numerator) is large and the cost (the denominator) is low, the agency therefore finds the corrective action with the best value to fix. Then, the agency sorts this column; the largest numbers have the largest impact or bang for the buck…the corrective action impact. But, these corrective actions with higher impact may not be the agency’s more important corrective actions. The rest of the exercise shows how to create a prioritization plan by relating the corrective action impact with the importance of the agency’s rank ordered corrective actions.

- In the breakout session the practical exercise averaged the corrective action compliance of several systems from the POA&M for each NIST 800-26 corrective action. Shouldn't these systems be weighted by importance of the systems in the Department-level prioritization?

  – No. The goal is to close a Department-level line item/corrective action. The systems are merely components of the line item. The average is showing what percentage has been corrected for the entire line item/corrective action. The line item in the spreadsheet also shows the cost of completing the compliance gap of ALL the systems with no regard to importance of the systems. Solving the problem of one system does not close the line item. Individual system importance is handled in the system-level prioritization part of the exercise and then overlaid onto the Department-level prioritization matrix to create a blended strategic action plan.

- Given the enterprise nature of most major systems and the increasing focus on sharing data between systems (intra & inter-agency), is it appropriate to address security issues regarding connectivity by incorporating by reference security plans for those other connected systems (e.g., LANs, shared databases, XML).

  – When the NIST Computer Security Expert Assist Team (CSEAT) reviews agencies, we look to ensure systems have a System Security Plan. If a system is interconnected, the system and the systems it interfaces with should have interconnection agreements and all systems should have security plans.

The following questions were raised during the afternoon session. Rather than speak for OMB colleagues, NIST opted to seek further clarification from OMB before responding the questions. Would a cost effectiveness analysis be appropriate rather than a cost benefit analysis for an OMB 300?

- What skill sets are required to develop an agency FEAF?

- In the CPIC timeline, at Planning Year (PY), should we also include some contract close outs?

- Does OMB believe that all NIST guidance is mandatory under FISMA? Or, is it only NIST guidance that is expressly made mandatory by the Secretary of Commerce?

- Will ST&E be required annually under FISMA (this will have to be incorporated into the POA&M process)?

- Are formal risk assessments (NIST 800-30) required under FISMA? OMB stated in A-130 Appendix III that risk assessments were not particularly useful (the agencies will have included formal risk assessments in POAMs).