FEDERAL COMPUTER SECURITY PROGRAM MANAGERS' FORUM

IT Security Metrics Workshop
A Practical Approach to Measuring Information Security:
Measuring Security at the System Level

Tuesday May 21, 2002

On May 21, 2002, the National Institute of Standards and Technology (NIST) and the Federal Computer Security Program Managers' Forum sponsored two IT Security Metrics Workshops designed to help Federal personnel with OMB FY 2002 Government Information Security Reform Act (GISRA) draft reporting guidance. Approximately 75 Federal government employees attended these workshops, where they learned to develop IT security metrics that align with NIST Special Publication (SP) 800-26 Self Assessment Guide for Information Technology Systems critical elements. This document captures the proceedings of these workshops, including the original metrics developed by breakout groups, a critique of each metric developed, and a corresponding ideal metric.

The ideal metrics, which were derived from the metrics the workshop participants developed, will be used as examples in the upcoming NIST Special Publication on Development and Implementation of System Security Metrics. The document will expand on the topics presented in the workshop and contain example metrics and implementation guidance for measuring the critical elements contained in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems." The document will be available for public review in September 2002.

Joan Hash of NIST introduced the workshop, followed by Marianne Swanson, Chair of the Federal Computer Security Program Managers' Forum. Marianne Swanson introduced the staff that would be supporting the workshop:

Nadya Bartol, Booz Allen Hamilton, IT Security Metrics Workshop Author and Trainer
Gail Brown, Booz Allen Hamilton, Breakout Group Facilitator
Ellen Roth, Booz Allen Hamilton, Breakout Group Facilitator
John Sabato, SAIC, Breakout Group Facilitator

Following introductions, Nadya Bartol began the training workshop. The workshop was designed in three modules:

- Metrics Development
- Breakout Session
- Metrics Program Implementation

The modules were created to address the following key learning objectives:

- Identify why metrics are important to IT security
- Understand the relationship between GISRA, NIST SP 800-26, and IT security metrics.
- Describe IT security metrics
- Describe the metrics development process
- Apply the metrics development process by creating metrics to be implemented at the system level
- Identify metrics-related roles and responsibilities
- Describe how to implement a metrics program

MODULE One: Metrics Development

Module One addressed the following learning objectives:

- Learn the definition and characteristics of IT security metrics
- Identify the difference between performance goals, performance objectives, and IT security metrics
- Learn the seven-step IT security metrics development process
- Discover the types of information and insights that can be gained from IT security metrics
- Demonstrate three examples of IT security metrics

MODULE TWO: Breakout Session

At the end of Module One, participants were grouped together for the breakout session. Each group developed a different metric that was extracted from the OMB GISRA Reporting Guidance. The groups were asked to fill out a Metric Form for the metric given by the facilitator, and then to brief the metric to the entire group after the Breakout Session was complete. The metrics in the following section are the metrics developed by the Breakout Groups.

While filling out the forms, participants were asked to determine what NIST SP 800-26 critical element and subordinate question related to the OMB metric, so that existing data from Self-Assessments could be used as data to answer the metric. Participants were asked to use critical elements in place of IT security performance goals and subordinate questions in place of IT security performance objectives. By going through this process, participants developed an understanding of the connection between performance goals, objectives, and metrics. For each metric, we have provided a short commentary on what was proposed by the Breakout Groups, a listing of any questions that surfaced about the metric, and an Ideal Metric Form that slightly modifies the proposed metrics for use in GISRA reporting for FY 2002.

Critical Element: 14.1 Is there a capability to provide help to users when a security incident occurs in the system?

Subordinate Question: 14.1.1 Is a formal incident response capability available?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.B.5.b:** Number of agency components with incident handling and response capability ____.
Purpose	To ensure that there is an incident response capability within the agency.
Implementation Evidence	Do all components have an incident response capability?
Frequency	Quarterly, but could be more or less frequent depending on activity.
Formula	Number of agency components that have incident response capability / # of components
Data Source	Information System Security Officer (ISSO) for a quarterly report of whether the capability has been implemented
Indicators	An upward trend is what we are looking for to reach 100%.

Comments:

This metric is a binary (Yes/No) metric, indicating the implementation rather than the efficiency and effectiveness of incident response. As noted by the group that produced this Metric Form, in very small agencies this is a very simple question. In very small agencies, a single office implements the incident response capability, which is used by the entire agency. In larger agencies, it may be necessary to ask each agency component whether they have an incident response capability in place.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.B.5.b:** Number of agency components with incident handling and response capability ____.
Purpose	To ensure that there is an incident response capability within the agency.
Implementation Evidence	1. Does your agency component maintain an incident response capability? Yes No 2. If the answer to question 1 is no, why not? Did not know of requirement Lack of resources Competing priorities
Frequency	Semi-annually
Formula	Number of agency components that have incident response capability / Total number of components
Data Source	ISSO, NIST SP 800-26 (particularly items 14.1 or 14.1.1)
Indicators	An upward trend with a goal of 100% is necessary to show progress and the continued strength of the IT security program. Question 2 is a causation question that points to the reason inadequate results occur. If the answer to question 2 is "Did not know of requirement" it may be necessary to investigate whether there is a policy in place requiring an incident response capability, or if guidance is necessary. Other corrective actions will be required if the answers to question 2 were "Lack of Resources" or "Competing Priorities."

Critical Element: 14.1 Is there a capability to provide help to users when a security incident occurs in the system?

Subordinate Question: 14.1.2 Is there a process for reporting incidents?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.B.5.c:** For FY01 and FY02, by agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported by each component.
Purpose	Determining number of successful incidents reported by component.
Implementation Evidence	1. Is there a process for reporting incidents? Yes No 2. If the answer to question 1 is no, then why not? _____. 3. Number of incidents reported by component. _____. 4. Number of successful incidents reported by component. _____.
Frequency	Monthly, but roll up these numbers for an annual total.
Formula	Number of incidents – successful = successful vs. unsuccessful incidents
Data Source	Incident response database, or incident response forms.
Indicators	A high number of successful incidents indicates weakness in the IT security program. One thing to consider: Is there inconsistency between components reporting? Why? It may be important to note the amount and type of training the system administrator is receiving and how this may be contributing to weaknesses that may be exploited. Also, consider whether there is an effective patch management system in place. This may help reduce successful incidents.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.B.5.c:** For FY01 and FY02, by agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported by each component.
Purpose	Determining number of successful incidents reported by component.
Implementation Evidence	1. Is there a process for reporting incidents? Yes No 2. If yes, what are the categories of incidents that you report? _____. 3. If the answer to question 1 is no, then why? Unaware of requirement Lack of resources Competing priorities 4. Number of incidents reported by component for each category _____.
Frequency	Monthly, and annually as a percentage of the total.
Formula	Successful incidents by component (possibly broken down for each category).
Data Source	Incident response database, or incident response forms.
Indicators	A high number of successful incidents indicates weakness in the IT security program. This metric can be correlated with a metric for system administrator training and with a metric for patch implementation. High numbers for this metric may indicate ineffectiveness or a lack of both system administrator training and patch implementation programs. Question 3 is a causation question. The answers to it point at possible reasons why incidents for the system are not reported, but does not provide insight regarding why percentages may be high.

Critical Element: 14.2 Is incident related information shared with appropriate organizations?

Subordinate Question: 14.2.3 Is incident information reported to FedCIRC, NIPC, and local law enforcement when necessary?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.B.5.d:** For FY01 and FY02, by agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.
Purpose	To validate that there is a process in place for reporting incidents to FedCIRC or law enforcement.
Implementation Evidence	1. There is a tracking system in place. 2. There is a database that you can get this information from.
Frequency	Information should be gathered as required to report to FedCIRC, with periodic summary. Data gathering should be done at the agency level.
Formula	Count of number of incidents reported externally to FedCIRC or law enforcement.
Data Source	Incident Response Team reports, database
Indicators	A program in place that reports incidents and tracks these incidents internally shows that a reporting process is in existence. If there is a reporting process, a count of reported incidents can be used to answer this metric.

Comments:

The Implementation Evidence portion of this Metric Form, as developed by the Breakout Group, lists things that will be in place and will be observable if there is a capability to report incidents to FedCIRC or law enforcement. However, it does not list specific questions that need to be answered via survey or through automatic data gathering to be able to calculate the metric.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.B.5.d:** For FY01 and FY02, by agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.
Purpose	To validate existence of a process for reporting incidents to FedCIRC or law enforcement.
Implementation Evidence	1. Is there a tracking system in place for reporting incidents to FedCIRC or law enforcement? Yes No 2. If the answer to question 1 is yes, is there a database that captures the incidents that have been reported? Yes No 3. If the answer to question 2 is yes, how many incidents were reported in FY01 ___ and FY02 ___? 4. If the answer to question 1 is no, then how is data captured? _____.
Frequency	Quarterly for the agency, and as required by FedCIRC in a summary.
Formula	Count of number of incidents reported externally to FedCIRC or law enforcement.
Data Source	Incident Response Team reports, Incident Reporting database
Indicators	A program in place that reports incidents and tracks these incidents internally shows that a reporting process is in existence. If there is a reporting process, a count of reported incidents can be used to answer this metric. This metric by itself does not necessarily indicate poor or excellent performance. A trend in this metric will provide a definite picture, but would not necessarily indicate a certain "appropriate" level of performance. Although an answer of "no" for question 1 is not preferable, the data sources yielded from question 4 may point to ways to gather the information without a tracking database. The Data Sources that are listed in the Metric Form are a great start for this scenario. If the answer to question 1 is "yes" and you have confidence that the Incident Response Team reports incidents internally and the database information is accurate (if available), then a count will be sufficient to calculate the metric.

Critical Element: 14.2 Is incident related information shared with appropriate organizations?

Subordinate Question: 14.2.3 Is Incident information reported to FedCIRC, NIPC, and local law enforcement when necessary?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.B.5.e:** Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance? What is the required average time to report to the agency and FedCIRC following an incident? __ agency, __ FedCIRC.
Purpose	To validate that incident reporting process is working and that required times to report incidents are being met.
Implementation Evidence	1. A program plan that shows that the policy is in place. 2. Reporting times and reporting criteria. 3. Records in database that has included the incidents, including how long it took to report. This implementation evidence validates that the process is working and meeting required times.
Frequency	Annually, as required for GISRA reporting.
Formula	
Data Source	Reports, database, tracking database. Reports generated by system owners. Survey responses.
Indicators	Reports are being made, and the times are available.

Comments:

The Implementation Evidence portion of this Metric Form lists elements that will exist if the agency and its components are sharing incident information with FedCIRC and how long the sharing process takes each time. The Metric Form brings up a great point: both policy and a program plan need to be in place to ensure that the agency and its components are aware of the requirement.

As noted by the group that produced this Metric Form, it will be necessary to reference OMB guidance to determine whether the agency and its components can answer "yes" to the first part of the metric, which asks whether sharing happens "in a timely manner consistent with FedCIRC and OMB guidance. This enables agencies to determine whether they should respond positively to the first question. Modifying the Implementation Evidence, while keeping in mind all the important points made in the current form under Implementation Evidence will yield specific questions that can be answered via survey or through automatic data gathering.

By answering the previous metric (Subordinate Question 14.2.3), you will know whether your agency is reporting to FedCIRC at all, and what data sources are available. Assuming a survey is administered to capture the data, the same questions will be posed to the same audience. To avoid duplication of effort, it is preferable to simply access a database or use another transparent data collection method rather than administer a survey. If a survey is the only realistic data gathering method, within the agency, special care should be taken to order the survey questions in a way that avoids duplication.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.B.5.e:** Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance? What is the required average time to report to the agency and FedCIRC following an incident? __ agency, __ FedCIRC.
Purpose	To validate that an incident reporting process exists.
Implementation Evidence	1. Does the agency use a tracking mechanism or database to capture incidents that are required to be reported to FedCIRC? Yes No 2. If the answer to question 1 is no, does agency policy state the average time required to share incident information within the agency and with FedCIRC? Yes No 3. If the answer to question 2 is yes, what is the required average time listed in agency policy for reporting to the agency _____ and to FedCIRC _____?
Frequency	Annually.
Formula	No formula necessary. The length and time to report to the agency and to FedCIRC should be extracted from agency policy.
Data Source	Incident response/reporting policy
Indicators	Availability of an answer indicates that the policy is detailed enough to specify upper limit of time within which incidents are to be reported internally to agency personnel and externally to FedCIRC. FedCIRC and OMB guidance can be referenced to determine what constitutes a "timely manner" so that the first part of this metric can be answered. Once you have the answer to question 3, then you can compare the average times listed in agency policy to those required in OMB guidance. If the time your agency is requiring for reports is not consistent with OMB guidance, then the policy should be modified to match OMB's times to gain compliance. If there is no agency policy in place, then you have identified a weakness in your agency's IT security program that should be corrected.

Critical Element: 1.2 Do program officials understand the risk to systems under their control and determine the acceptable level of risk?

Subordinate Question: 1.2.1 Are final risk determinations and related management approvals documented and maintained on file?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.a:** Number and percentage of systems that have been assessed for risk. FY01 _#_ and _%__, FY02 _#_ and _%_.
Purpose	To quantify the # of total systems in compliance of requirement for risk assessments, and to measure improvement in status from FY01-FY02. This is a GISRA requirement.
Implementation Evidence	
Frequency	Agency-dependent. Annual review and adjustment as required. OMB A-130.
Formula	At Agency level: Risk Assessments on File / IT systems in inventory (inventory database)
Data Source	Inventory of IT systems that include all Major Applications and General Support Systems.
Indicators	Monitors existence and currency of risk assessments. Measures compliance with agency policy regarding content of risk assessments. Example: Rules of Behavior, has risk assessment been conducted, is a contingency plan available, did this lead to Certification & Accreditation (C&A)?

Comments:

The Purpose listed by the Breakout Group for this element is excellent, since it recognizes that it is a good practice to identify changes in IT security elements from year to year. The Breakout Group did not provide implementation evidence for this metric.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.a:** Number and percentage of systems that have been assessed for risk. FY01 _#_ and _%__, FY02 _#_ and _%_.
Purpose	To quantify the # of total systems in compliance with the requirement for risk assessments, and to measure improvement from FY01-FY02.
Implementation Evidence	1. Does your agency maintain a current inventory of IT systems? Yes No 2. Does your agency have a record of IT systems from FY01? Yes No 3. If yes, how many systems are/were there in your agency (or agency component, as applicable)? FY01 ____. FY02 ____. 4. How many IT systems have been assessed for risk? FY01 ____. FY02 ____.
Frequency	Annually, semi-annually
Formula	At Agency level: Risk Assessments on File / IT systems in inventory (inventory database)
Data Source	Inventory of IT systems that includes all Major Applications and General Support Systems, Risk Assessment Repository.
Indicators	This metric monitors existence and currency of risk assessments. Since this metric deals with risk to systems, it is especially important to monitor trends, since an upward trend in risk indicates deterioration of agency IT security overall.

Critical Element: 1.2 Do program officials understand the risk to systems under their control and determine the acceptable level of risk?

Subordinate Question: 1.2.1 Are final risk determinations and related management approvals documented and maintained on file? 1.2.2 Has a mission/business impact analysis been conducted?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.b:** Number and percentage of total systems that have been assigned a level of risk, e.g. high, medium, or basic. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	Does the organization have an inventory of systems? Is it current? Have risk assessments been done? Have Business Impact Assessments (BIAs) been conducted
Implementation Evidence	1. Does the agency maintain an inventory of systems? Yes No 2. Is it current? Yes No 3. Have risk assessment been done for all of these systems? Yes No 4. Have BIAs been conducted? Yes No
Frequency	Quarterly self-assessment, annual report of results
Formula	FY 01 statistics vs. FY 02 statistics to measure progress
Data Source	BIAs on file, risk assessments, inventory lists, Certification & Accreditation on applications
Indicators	To obtain information to determine what is the acceptable level of risk managers are responsible for. Assess risk and determine the impact on the organization.

Comments:

The data to complete this metric requires a system inventory. Questions 1 and 2 for Implementation Evidence may not be necessary if system inventory questions are asked in related metrics questions. Question 4 of Implementation Evidence assumes that if a BIA is conducted, then a level of risk as been assigned. This is generally true, but remember to make sure that the results of the BIAs are recorded for

each system. NIST self-assessments from NIST SP 800-26 will be a rich data source to gather some of the information required to answer this metric.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.b:** Number and percentage of total systems that have been assigned a level of risk, e.g. high, medium, or basic. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To gauge the level of accountability for accepting security risks within an agency.
Implementation Evidence	1. Does the agency maintain an inventory of systems? Yes No 2. Is it current? Yes No 3. How many systems have had risk assessments performed? _____ 4. Of the systems that have had risk assessments performed, how many have been assigned a level of risk? FY01 ___ FY02 ___.
Frequency	Quarterly self-assessment, annual report of results
Formula	Answer to Question 4 / # of Total Systems
Data Source	BIAs on file, risk assessments, inventory lists, Certification &Accreditations on systems
Indicators	High numbers and upward trends are very desirable for this metric. Low or declining numbers indicate that the results of risk assessments are not used for the reduction of risk determination and that agency officials are not accepting accountability for security.

Critical Element: 5.2 Is the plan kept current?

Subordinate Question: 5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.c:** Number and percentage of total systems that have an up-to-date security plan. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To quantify the # of total systems in compliance with the requirement for security plans; measure improvement from FY01-FY02.
Implementation Evidence	Answers to NIST SP 800-26 Subordinate Questions 5.1.1-5.1.3: 5.1.1 Is the system security plan approved by key affected parties and management? Yes No 5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? Yes No 5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? Yes No
Frequency	Agency-dependent. Annual review and adjustment as required. OMB A-130.
Formula	At Agency level: # of plans in place / IT systems in inventory (inventory database)
Data Source	Inventory of IT systems that include all Major Applications and General Support Systems.
Indicators	Monitors existence and currency of security plans. Measures compliance with agency policy regarding content of security plans. Example: Rules of Behavior, has risk assessment been conducted, is a contingency plan available, did this lead to C&A?

Comments:

The Breakout Group's Metric Form makes maximum use of existing data sources by noting that the answers to NIST SP 800-26 self assessments provide the information needed to answer this metric. It is always preferable to use existing data to answer metrics, as it relieves the burden from you and from those individuals one would normally ask for data. Keep in mind that data may have changed or been updated since the self-assessment was performed. The self-assessment is a rich data source, but it may be necessary to check for these updates or validate the data from the self-assessment.

If the questions in the Implementation Evidence portion of the Metrics Form are used exactly as written, one will have to ask the same question for each system, or aggregate data from self-assessment forms for all the systems in the agency. Not all systems may have undergone the self-assessment process. Make sure you are aware of what data you have and how this data compares to the number of systems in the agency's system inventory.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.c:** Number and percentage of total systems that have an up-to-date security plan. FY01 _#_ and _%_, FY02 _#_ and _%_. Number and percentage of systems with current security plans in place.
Purpose	To quantify the total number of systems in compliance with the requirement for having a security plan, and measure improvement from FY01-FY02.
Implementation Evidence	1. How many systems are there in your agency (or agency component, as applicable)? _____. 2. For each system, is the system security plan approved by key affected parties and management? Yes No 3. For each system, does the plan contain the topics prescribed in NIST Special Publication 800-18? Yes No 4. For each system, is a summary of the plan incorporated into the strategic IRM plan? Yes No *Note: Questions 2-4 are NIST SP 800-26 subordinate questions (objectives).
Frequency	At least annually.
Formula	At agency level: # of plans in place / # of IT systems in inventory (inventory database). The same formula should be used at the agency component level, and answers should be combined to calculate the agency total.
Data Source	Inventory of IT systems that includes all Major Applications and General Support Systems, 800-26 Self Assessments
Indicators	This metric monitors existence and currency of security plans.

Critical Element: 4.1 Has the system been certified/recertified and authorized to process (accredited)?

Subordinate Question: 4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.d:** Number and percentage of total systems that have been authorized for processing following certification and accreditation. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To determine the number of systems that are certified and authorized, and whether the organization conducts C&A.
Implementation Evidence	1. Does your agency (or agency component, etc) maintain a complete and up to date inventory of systems? Yes No 2. Is there a C&A process within your agency? Yes No 3. Where is the data repository for systems that are subject to C&A? _____.
Frequency	Quarterly
Formula	Number of systems that have been Certified and Accredited / Number and percentage of systems total
Data Source	System Inventory, C&A Records
Indicators	This is a measure of compliance or existence of a C&A process. The goal is 100%, and a positive trend should be upward. C&A shows if there are known vulnerabilities and when they will be fixed.

Comments:

The Metric the Breakout Group developed addresses the issue of whether a C&A process is used within the agency. However, the Implementation Evidence provided does not fully answer the GISRA Guidance Question, which asks for a number and percentage of total systems that have been authorized for processing. The Implementation Evidence may lead one to a repository from which you could extract the number and percentage, but it does not directly collect this information through a survey question.

Ideal Metric:

Metric	**GISRA Guidance Question II.C.1.d:** Number and percentage of total systems that have been authorized for processing following certification and accreditation. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To determine the percentage of systems that are certified and accredited.
Implementation Evidence	1. Does your agency (or agency component, etc) maintain a complete and up to date inventory of systems? Yes No 2. Is there a C&A process within your agency? Yes No 3. How many systems are registered on the system inventory? FY01 ___. FY02 ___. 4. How many systems received full certification and accreditation in FY01 ___. FY02 ___.
Frequency	Quarterly
Formula	Number of systems that have been Certified and Accredited / Number and percentage of systems total
Data Source	System Inventory, C&A Records
Indicators	This is a measure of compliance or existence of a C&A process. The goal is 100%, and a positive trend should be upward. C&A shows that the system has been thoroughly assessed for risk and that an agency official accepts full responsibility for the security of a system.

Critical Element: 4.1 Has the system been certified/recertified and authorized to process (accredited)? 4.2 Is the system operating on an interim authority to process in accordance with specified authority?

Subordinate Question:

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.e:** Number and percentage of total systems that are operating without written authorization (including the absence of certification and accreditation). FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To quantify degree of potential risk from unaccredited systems.
Implementation Evidence	1. Does your agency (or agency component, as applicable) maintain a complete and up-to-date inventory of systems? Yes No 2. If the answer to question 1 is yes, how current is the existing inventory. _____. 3. How frequently is this inventory updated? _____. 4. Of the inventory, how many are certified and uncertified? Certified ____. Uncertified ____.
Frequency	Equal to certification period, which may be yearly or every three years.
Formula	Number of certified systems / total number of systems (yields %) Number of uncertified system / total number of systems (yields %)
Data Source	Security program manager, certification repository, computer security plans, change management process
Indicators	This metric provides evidence of the certification process and compliance with certification procedures. Any number of underlying events might surface.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.e:** Number and percentage of total systems that are operating without written authorization (including the absence of certification and accreditation). FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To quantify degree of potential risk from unaccredited systems.
Implementation Evidence	1. Does your agency (or agency component, as applicable) maintain a complete and up-to-date inventory of systems? Yes No 2. If the answer to question 1 is yes, how current is the existing inventory. _____. 3. How frequently is this inventory updated? _____. 4. How many systems are in your agency (or agency component)? FY01 ___. FY02 ___. 5. How many systems in your agency (or agency component) are certified? FY01 ___. FY02 ___. How many are uncertified? FY01 ___. FY02 ___. 6. How many of the uncertified systems are operating with an Interim Authority to Operate (IATO)? FY01 ___. FY02 ___.
Frequency	Quarterly
Formula	Number of uncertified systems from Question 5 / Total number of systems in inventory from Question 4
Data Source	Security program manager, certification repository, computer security plans, change management process
Indicators	A downward trend is necessary for this metric, and the goal is to have 0% operating without a written authorization. Agencies that have a C&A process but are not reaching 0% or a low percentage number will need to examine why the C&A process is not working, and assess the security risks that are present because systems are operating without C&A. Question 6 adds additional documentation. While OMB did not request that the agencies quantify and report the number of systems under IATO, quantifying this information demonstrates some program movement toward full accreditation.

Critical Element: 3.1 Has a system development life cycle methodology been developed?

Subordinate Question: 3.1.2 Does the business case document the resources required for adequately securing the system? 3.1.3 Does the Investment Review Board ensure investment requests include the security resources needed?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.f:** Number and percentage of total systems that have the costs of their security controls integrated into the life cycle of the system. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To quantify security costs identified throughout the system development life cycle.
Implementation Evidence	1. How many systems are there in your organization (or agency component, etc)? _____ 2. Do you have a formal SDLC? Yes No 3. If the answer to question 2 is no, why not? Unaware of requirement Lack of resources Competing priorities 3. Does the SDLC track the cost of security controls? Yes No 4. How many systems are in or went through the SDLC? _____.
Frequency	Annually
Formula	# of systems /# of systems having gone through SDLC (FY01, FY02)
Data Source	Budget process data (Exhibit 300), Review of security plans
Indicators	High percentage would show security resources allocated for each system during the life cycle.

Comments:

The Implementation Evidence for this Metric Form should give comprehensive information to calculate the metric, and identify why an SDLC has not been developed in those agencies or agency components that answer "no" to question 1. The number answer to this metric will be the answer to question 4. The percentage will be the answer to question 4/answer to question 1.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.f:** Number and percentage of total systems that have the costs of their security controls integrated into the life cycle of the system. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To quantify the percentage of systems that are in compliance with the OMB requirement to integrate security costs into the system lifecycle.
Implementation Evidence	1. How many systems are there in your organization (or agency component, etc)? _____ 2. Do you have a formal SDLC? Yes No 3. If the answer to question 2 is no, why not? Unaware of requirement Lack of resources Competing priorities 3. Does the SDLC track the cost of security controls? Yes No 4. Does the SDLC process incorporate the cost of security at every step as required? Yes No 5. How many systems are in or went through the SDLC? FY01____ FY02 ____.
Frequency	Annually
Formula	# of systems /# of systems having gone through SDLC (FY01, FY02)
Data Source	Budget process data (Exhibit 300), Review of security plans
Indicators	The goal for this metric is to show an upward trend. High percentage would show that security resources are allocated for each system during the life cycle, which is the ideal state for system development. Questions 2 and 4 quantify the organization's eligibility to report a positive result for this metric. Question 3 is a causation question that points at possible solutions to evidence that the agency implements a formal SDLC process.

Critical Element: 2.1 Have the security controls of the system and interconnected systems been reviewed?

Subordinate Question: 2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.g:** Number and percentage of total systems for which security controls have been tested and evaluated in the last year. FY01 _#_ and _%_, Fy02 _#_ and _%_.
Purpose	Measure level of compliance with requirement for system testing.
Implementation Evidence	1. Do you have a system inventory? Yes No 2. If not, why? _____. 3. Do you use automated tools such as Bindview or ESM? Yes No 4. How often do you run these tools? _____
Frequency	Annually
Formula	# of systems tested / total # of systems in the inventory
Data Source	OMB 53, 300 (Exhibits), budget office. Audits, C&A database, automated tool reports
Indicators	The percentage trend should increase and approach or equal 100%. Fewer penetrations = fewer audits, fewer combinations of incident types.

Comments:

The Breakout Group Metric Form takes a creative approach to discovering the data by asking whether automated tools are used, and how often the tools run. However, the data that will result from the Implementation Evidence questions will not answer the metric—it will simply yield data about whether security controls are tested in general. To correct this, it is necessary to find out whether security controls are tested for each system. This data will need to be gathered from audit results or directly from system owners. Data validation will be difficult unless a data source is available that reliably records when system tests are conducted.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.g:** Number and percentage of total systems for which security controls have been tested and evaluated in the last year. FY01 _#_ and _%_, Fy02 _#_ and _%_.
Purpose	Measure level of compliance with requirement for system testing.
Implementation Evidence	1. Do you have a system inventory? Yes No 2. How many systems run automated auditing tools regularly (at least quarterly) in FY01___ FY01 ____. 3. How many systems underwent penetration testing in FY01 ___ and FY02 ___. 4. How many systems underwent security test and evaluation (ST&E) in FY01 ___ and FY02 ___. 5. How many systems conducted one or more of the activities that are the answer to questions 2-4 in FY01 ___? FY02 ___?
Frequency	Annually
Formula	# of systems tested (Question 5) / total # of systems in the inventory
Data Source	OMB Exhibits 53 and 300, budget office. Audits, C&A database, automated tool reports
Indicators	The percentage trend should increase and approach or equal 100%. Fewer successful penetrations should result in fewer audits and change the incident types in the long run. Overall, it is important that security controls are tested once they are in place to make sure they are working as proposed. As things change within the security environment, what is necessary as a control also may change. To keep up, regular testing and evaluation of controls should be conducted.

Critical Element: 9.2 Has a comprehensive contingency plan been developed and documented?

Subordinate Question: 9.2.10 Has the contingency plan been distributed to all appropriate personnel?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.h:** Number and percentage of total systems that have a contingency plan. FY01 _#_ and _%_, FY02 _#_ and %_.
Purpose	To determine actual percentages relative to the desired state. For contingency plans, the desired state would be 100%.
Implementation Evidence	1. Is there a contingency plan required of all systems. Yes No 2. How many systems are there? _____ 3. Is the contingency plan documented for each system? Yes No
Frequency	Annually.
Formula	# = total systems, %: Total with plan/Total systems
Data Source	Database, inventory tracking system
Indicators	Availability of information is improved when systems are covered in a contingency plan. Contingency plan supports business continuity and achieving goals.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.h:** Number and percentage of total systems that have a contingency plan. FY01 _#_ and _%_, FY02 _#_ and %_.
Purpose	To determine the percentage of systems in compliance with the requirement to have a contingency plan. Existence of such a plan indicates a certain level of preparedness if the plan were to be activated.
Implementation Evidence	1. How many systems are there in your agency? _____ 2. How many systems have a contingency plan? _____
Frequency	Annually.
Formula	# = Total Systems, %: Total with plan/Total systems
Data Source	Database, inventory tracking system
Indicators	The desired state for this metric would be that 100% of systems have a contingency plan. An upward trend is positive. A low percentage of systems having contingency plans may indicate a lack of agency policy requiring contingency plans.

Critical Element: 9.3 Are tested contingency/disaster recovery plans in place?

Subordinate Question: 9.3.3 Is the plan periodically tested and readjusted as appropriate?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.C.1.i:** Number and percentage of total systems for which contingency plans have been tested in the past year. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To determine the number and percent of contingency plans tested in the past year.
Implementation Evidence	1. How many systems do you have within your agency (or agency component? _____ 2. How many of the systems have a tested contingency plan? _____
Frequency	Annually.
Formula	Number of contingency plans tested / Number of systems total (Answer to question 2) / (Answer to question 1) = %
Data Source	Contingency plan repository. All contingency plans should be held by one group/person, or by system managers.
Indicators	If the metric yields a low percentage, it identifies the specific system for follow up and retesting, development of a contingency plan, or analysis of where the contingency plan is lacking.

Comments:

The Data Source portion assumes that there is a contingency plan repository within the agency. If there is a repository, it may be possible to bypass asking Implementation Evidence survey questions of specific individuals. If there is no repository, then the survey questions will likely need to be asked of system owners.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.C.1.i:** Number and percentage of total systems for which contingency plans have been tested in the past year. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To determine the number and percent of contingency plans tested in the past year.
Implementation Evidence	1. How many systems do you have within your agency (or agency component? _____ 2. How many of the contingency plans have been tested within the last year? _____
Frequency	Annually.
Formula	Number of contingency plans tested / Number of systems total (Answer to question 2) / (Answer to question 1) = %
Data Source	Contingency plan repository. All contingency plans should be held by one group/person, or by system managers.
Indicators	If the metric yields a low percentage, it identifies specific systems for follow up and retesting, development of a contingency plan, or analysis of where the contingency plan is lacking.

Critical Element: 13.1 Have employees received adequate training to fulfill their security responsibilities?

Subordinate Question: 13.1.2 Are employee training and professional development documented and monitored?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.D.1.f:** For FY01 and FY02, number of employees with significant security responsibilities that received specialized training. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To maintain their knowledge and skills for designated security roles and security responsibilities for specific systems.
Implementation Evidence	1. How many employees in your agency (or agency component, etc) have significant security responsibilities? _____. 2. Are training records maintained? Yes No 3. How many training plans state that specialized training is necessary? _____. 4. How many of those with significant security responsibilities have received the required training stated in their training plan? _____.
Frequency	Annually at minimum, and more often as needs dictate.
Formula	Answer to Question 4/Answer to Question 1
Data Source	Employee training records, Database, Course completion certificates
Indicators	If level of vulnerabilities is constant or decreases, or security incidents/unauthorized incidents have decreased, this means skills and abilities have increased.

Comments:

This Metric Form is comprehensive. It should be very effective in helping calculate the metric.

One item to note is that the definition of "significant" security responsibilities may vary from agency to agency. It may be necessary to define this term clearly before starting to gather information, so that the term is applied uniformly throughout the data collection in your agency. You may also need to define what "specialized" training is required for such personnel.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.D.1.f:** For FY01 and FY02, number of employees with significant security responsibilities that received specialized training. FY01 _#_ and _%_, FY02 _#_ and _%_.
Purpose	To gauge the level of expertise among designated security roles and security responsibilities for specific systems within the agency.
Implementation Evidence	1. How many employees in your agency (or agency component, etc) have significant security responsibilities? _____. 2. Are training records maintained? (Training records indicate the training that specific employees took). Yes No 3. How many training plans state that specialized training is necessary? _____. 4. How many of those with significant security responsibilities have received the required training stated in their training plan? _____.
Frequency	Annually at minimum.
Formula	Answer to Question 4 / Answer to Question 1
Data Source	Employee training records or database, course completion certificates
Indicators	This metric can be correlated with the number of security incidents and the number of patched vulnerabilities to determine if an increase in trained security staff is related to and facilitating a reduction in certain types of incidents and open vulnerabilities.

Critical Element: 13.1 Have employees received adequate training to fulfill their security responsibilities?

Subordinate Question: 13.1.2 Are employee training and professional development documented and monitored?

Breakout Group Proposed Metric Form:

Metric	**GISRA Guidance Question II.D.1.g:** Briefly describe what types of security training were available during the reporting period, and for FY01 and FY02, the total costs of providing such training. FY01 ___ and FY02 ___.
Purpose	To quantify degree of potential risk from unaccredited systems.
Implementation Evidence	List of training courses, cost of training per student
Frequency	Semi-annually
Formula	Sum of cost per student / # of students
Data Source	SF-182, other agency forms, ISS PM or HRM department personnel
Indicators	Training program is crucial to an agency security program. Lack of funding in available training could place systems in continued risk of security problems.

Ideal Metric Form:

Metric	**GISRA Guidance Question II.D.1.g:** Briefly describe what types of security training were available during the reporting period, and for FY01 and FY02, the total costs of providing such training. FY01 ___ and FY02 ___.
Purpose	To quantify annual costs of security training and observe trends of these costs.
Implementation Evidence	1. What was/is the security training budget for your agency (or agency component as applicable)? FY01 ____. FY02 ____. 2. Do budget records record the cost of security training per course? Yes No 3. Do budget records record the cost of security training per student? Yes No
Frequency	Semi-annually
Formula	Budget totals for FY01 and FY02.
Data Source	SF-182, other agency forms, ISS PM or HRM department personnel
Indicators	Training program is crucial to an agency security program. Lack of funding in available training could place systems in continued risk of security problems. The trend in an agency training budget can be compared with a trend in incidents caused by uneducated users to determine whether an increase in training budget reduces these incidents. Questions 2 and 3 go above and beyond the GISRA question. However, they may help identify shortfalls in the training and provide data for lower level metrics.

MODULE THREE: Metrics Program Implementation

In this module, participants:

- Received an introduction to IT security metrics-related roles and responsibilities
- Learned the steps involved in IT security metrics program implementation by learning the process and following an example through the process