APPROACHES TO SECURITY METRICS

A Report of the Workshop Held June 13-14, 2000 at the
National Institute of Standards and Technology (NIST)
In conjunction with the
Computer System Security and Privacy Advisory Board (CSSPAB) Meeting

Fran Nielsen, NIST

Abstract

This report summarizes a workshop to map information technology (IT) security metrics activities. The workshop was a collaboration of the National Institute of Standards and Technology (NIST) and the Computer System Security and Privacy Advisory Board (CSSPAB). Several formal briefings on metric-related activities were given. Two panel sessions discussed practices in government and industry to measure security. Questions to help guide follow-on activities are presented.

1. Introduction

Increased reliance on IT systems and interconnection mean increased concern about the security of interconnecting those systems. A plethora of security incidents, such as denial of service, have been widely publicized. New attacks are reported daily. System owners and users react to this news by rushing to acquire the latest "cure." Do these efforts result in more secure systems? If so, how do system owners and users know this? What makes an effective security program? How are effective security programs measured?

Determining how well we are protecting information system assets is difficult, because there are no commonly accepted approaches to measuring security. Security metrics are needed to understand the current state-of-security, to improve that state, and to obtain resources for these improvements. A major problem is the diversity of meanings given to security metrics and the ambiguity surrounding them.

On June 13 and 14, 2000, NIST and CSSPAB convened a workshop to discuss security metrics. The workshop was seen as a starting point to continue cataloging and developing measures for determining the effectiveness of Federal security programs.

1.1 Workshop Background

In November 1998, the NIST Director, Mr. Raymond Kammer, wrote the CSSPAB a letter (appendix 1) in which he requested input on security focus areas. The Board responded with a decision to convene a workshop on security metrics.

1.2 Workshop Goal and Objectives

The goal of the initial workshop was to assess current information infrastructure protection metrics by identifying security metrics and their uses and then to determine the existence of any voids. The objectives of the workshop were twofold: to bring together interested parties to discuss the broad issue of security metrics and to collate the various approaches to defining and using security metrics.

The Board compiled several questions to be explored during the workshop:

- What are the different definitions of "security metrics?"
- What are measures of security against specific security threats?
- What are overall system security measures?
- What are some qualitative measures, e.g., adherence to "standards" or checklists of practices?
- What are real-time measures of security in extended networks?
- What are some uses of statistically-sampled data in measurement systems?
- What are some areas where metrics are lacking?
- What are ways to effectively communicate metrics, assurance levels and risk management tradeoffs to executives, lawmakers, and the public so that risks and protections are properly understood in both business and public policy terms?

1.3 Workshop Format

The focus of the workshop was security metrics for non-classified systems. While the workshop was open to all interested parties, a number of individuals were specifically invited to attend and encouraged to join in discussions. A list of workshop participants is provided at the end of this report.

Day one of the workshop was comprised of briefings on various metrics activities, including the GAO's audit procedures, the CIO Council's Security Assessment Framework, and the DOD's Information Assurance Readiness project. Day two consisted of two case-study panel sessions, one for government and one for industry, with significant interaction from audience participants. Government panel members from GAO, Customs, USAID, and USDA and industry panelists from Citigroup, First Union, Dupont, and General Motors discussed measures used in their organizations.

1.4 Report Format

Four major sections follow this introductory information. In the first section, each formal briefing is summarized, including discussion from workshop participants. The second section describes the two panel sessions and covers, in general, the discussion during these sessions. The appendices contain the briefing slides and supporting materials used by the speakers as well as any presentation aids used by the panelists. The third section

presents a new set of questions based on workshop dialogue. The final section contains summary remarks.

2. Workshop Briefings

2.1 What are Security Metrics?

Dr. Stuart Katzke, National Security Agency, set the stage for the workshop with his presentation summarizing the problem. He emphasized that the discipline of security metrics is essentially immature. He pointed out the ambiguity surrounding the concept, noting the different meanings and uses of "security metrics." For example, security metrics are key in testing, evaluation, assessment, accreditation, training, intrusion detection, observance, and performance. They relate to requirements, specifications, best practices, and baselines. There are direct and indirect methods of getting to the answer of "how secure is it?"

In response to a question from Mr. Frank Reeder, The Reeder Group and CSSPAB Chairman, about potential gaps in efforts to develop security metrics, Dr. Katzke pointed out that gaps exist almost everywhere. He said contributions toward clarifying the ambiguity and focusing the many diverse activities would be a good start.

Dr. Katzke stressed the importance of system-wide or enterprise-wide assessments. What has been done so far tends to focus on module and component testing. In fact, many groups are examining and assessing security products and technologies, such as firewalls and smart-cards. What happens when these are put together and attached to a network? Currently this type of security assessment is missing; yet, it is vitally important.

Mr. Richard Guida, U.S. Department of the Treasury and CSSPAB member, suggested that the ISO standard for the Common Criteria (CC) has a good example of a security metrics process that might be appropriate for this more encompassing perspective. Mr. Guida pointed out, however, that the CC is only a part of the answer to the metrics question. Dr. William Mehuron, Director of NIST's Information Technology Laboratory, pointed out the need to create a business case for the adoption of the CC and suggested using the BITS approach. The Banking Industry Technology Secretariat (BITS) was created as a strategic and technical arm for the financial services industry in the e-commerce arena. The goals of BITS are to:

- Facilitate the growth of electronic banking and financial markets,
- Facilitate development of superior, market-driven technology,
- Maintain the industry's role at the heart of the payments system as e-commerce evolves,
- Sustain consumer confidence and trust by ensuring the safety, soundness, privacy and security of financial transactions, and
- Leverage resources and infrastructure across the industry (see www.bitsinfo.org for information on BITS).

Mr. Joseph Leo, Chief Information Officer (CIO) at the U.S. Department of Agriculture and CSSPAB member, reminded the workshop that a link exists between dollars and measures so any approach devised should address cost of security.

2.2 The Defense-wide Information Assurance Program (DIAP)

Mr. Terry Bartlett, U.S. Department of Defense (DOD), described the information assurance readiness project. The project's objective is to assess the state of operational information assurance (IA) across the DOD. One of the first key steps is the definition of metrics and criteria for applying them, including an IA process that should be flexible and relevant. The metrics themselves need to be consistent and widely understood, on a level with measures such as the Dow Jones Industrial Average, the Gross Domestic Product, and the Consumer Price Index.

The process involves rolling up information obtained from each organizational unit and subunit. The data will be collected and trends will emerge leading to metrics. The project will develop the business case and the methodology for assessing IA damage. Mr. Bartlett predicts a three-year effort on this program, resulting in better analysis for forecasting capabilities and effectiveness. Asking rhetorically "how effective is it and how much does an ounce of protection cost," Mr. Bartlett pointed out the lack of analyzing "security effectiveness." Mr. Daniel Knauf, National Security Agency and CSSPAB member, also suggested that "protection" is another nebulous term. Mr. Bartlett commented that protection is a combination of people, technology, and policy and he said that metrics will be defined by policy. When subjective measures are decided, these can become agreed objective measures.

Some of the challenges facing the project are that no commonly accepted IA metrics exist and the IA process (e.g., review versus audit) has not been agreed. Another key concern, and an area requiring assistance, is how to do a better job of measuring end-to-end systems. It was observed that it would be beneficial if the work of the national security community could be shared with the civilian side.

2.3 The Systems Security Engineering Capability Maturity Model (SSE-CMM)

Mr. George Jelen, International Systems Security Engineering Association (see www.issea.org), gave a brief history of the SSE-CMM project. The maturity model is seen as an overall metric; that is, it is considered a metric in and of itself. The SSE-CMM is an appraisal methodology measuring two dimensions: process and security. The model describes characteristics to ensure good security engineering by capturing industry best practices and by defining a continuous improvement approach.

Mr. Jelen also reported on a current Information Assurance Technology Assessment Center (IATAC) research effort to define a metrics development process. This approach describes the relationship between process and security metrics. For example, sample process metrics for internal access control are: frequency of reviews and percent of users

meeting password policy. Sample security metrics for access control are: number of failed login attempts and number of virus infections.

Mr. Jelen's presentation highlighted the difference between measurements and metrics. Measurement is one-time view of specific parameters represented by numbers, weights, or binary statements. Metrics are produced by taking measurements over time and comparing two or more with a predefined baseline. Metrics must be SMART – specific, measurable, attainable, repeatable, and time-dependent.

In response to Mr. Leo's comments about the complexity of measuring a moving target, given the rapid pace of technology changes and the fact that there is no "state," Mr. Jelen confirmed the challenge and pointed out that the intent of SSE-CMM is to define ways of measuring security "goodness" wherever it occurs. Mr. Jelen encouraged the tailoring of security controls in response to asking "What is my worst security nightmare?" Mr. Jelen views the work as top down risk assessment and an area for further research.

2.4 Federal Chief Information Officers' Council (CIO) IT Security Assessment Framework

Mr. John Gilligan, Chief Information Officer (CIO) of the Department of Energy, described the CIO Council's work to produce a high-level management tool for agencies to assess the health of their IT security programs. Mr. Gilligan emphasized that a key issue is getting management to understand that IT security is a strategic resource. The problem is how to tell them what is enough security. He also stressed the change from looking at security from a systems and networks perspective to a site or enclave view. He emphasized that the strengths of the Framework are that it is based on existing mandates and guidance and it can be implemented now.

The IT Security Assessment Framework was developed by NIST for the CIO Council's Committee on Security Privacy and Critical Infrastructure Protection. The purpose of the Framework is to give Federal managers a way to ascertain, through self-assessment or outside review, the state of their security management and, if necessary, to take steps to make improvements.

Based on established mandates (such as the Computer Security Act of 1987 and the Clinger-Cohen Act of 1996), requirements (e.g., OMB Circular A-130 Appendix III), and guidance (e.g., NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP)), the Framework separates measurement criteria into 5 levels based on risk assessment, completeness and effectiveness of security controls.

Mr. Gilligan indicated that the impetus for the development of the Framework was discussion with Congressman Steve Horn's staff about grading agencies on how well IT security programs are managed.

2.5 An Audit-based Approach to Information Security Metrics

Ms. Jennifer Bayuk, Bear, Stearns, and Company, described an audit-based approach to measuring the effectiveness of information systems security. Ms. Bayuk's work incorporates industry standard control objectives and industry best practices with a locally-defined, systems security framework. This approach uses audit steps as a basis for metrics that result in recommendations for improvements. The organization determines its control objectives and the methodology for implementing them depends on the organizational culture, its structure, its resources, and its environment. The approach also allows an organization (or an independent testing organization) to measure security effectiveness.

A clear statement of the objectives for security controls is key to measuring security effectiveness. These objectives reflect the security consciousness of an organization. That is, it is assumed that an organization that makes the effort to adopt formal control objectives takes security seriously and manages its risks.

Once the organization has determined its objectives, it creates its own system control framework, dividing activities into six processes: policy, awareness, implementation, monitoring, compliance, and strategy. These processes industry standards are taken from the Control Objectives for Information and Related Technology Framework (COBIT), issued by the Information Systems Audit and Control Association (ISACA) (see www.isaca.org). These objectives have a standard unit of measure in the Information Systems Audit. Audit steps specify the actions that an auditor will take to independently gather evidence of activities contributing to the control objective. Two calculations are performed: one against the standards and one against the organization's own objectives. The calculations are based on the percentage of audit steps passed for the control objective (i.e., standards) and for the framework process (i.e., own goals).

Because the metrics compare industry standard objectives, they make it possible to compare the security environments at two different organizations. These metrics use management's own selection of control objectives.

2.6 An Overview of the General Accounting Office's Federal Information System Computer Audit Manual (FISCAM)

Mr. Darrell Heim, General Accounting Office (GAO), reviewed the contents of the FISCAM, the manual used when auditing Federal IT security programs. Legislation for better controls over critical assets and operations (e.g., the "CFO Act") was the impetus for GAO creating FISCAM. While FISCAM was developed to support financial statements, it has recently been used during non-financial audits.

The chapter on IT security covers six control areas: entity-wide security program planning and management, access control, application software development and change control, system software, segregation of duties, and service continuity. The focus of the review initially is on general control analysis. If weaknesses are found in general, then

there is no need to look at application controls, because general weaknesses must be overcome first.

Mr. Heim stressed that GAO is working with individuals in the agencies to find problems and recommend fixes. He said that he had seen a "dwindling down" of general weaknesses; however, agencies must be aware of controls significant to applications.

In response to discussion on the purpose of GAO's penetration testing and the use of FISCAM, Mr. Heim noted that Presidential Decision Directive 63 (PDD63) is an example of increased attention to the important issue of IT security and the nation's information infrastructure.

2.7 Quantitative Risk Assessment

Mr. Fred Tompkins, Key Technologies and Security, Inc., advocated a "close enough" approach for security metrics, suggesting that risk analysis should be the metric for determining the effectiveness of security programs. Risk management is an analytical process; however, the focus has been on numbers rather than on this process. Acceptable risk is qualitative (e.g., high, medium, low); yet, managers are faced with quantifying it. He said that "planning is what is important, not the plan." Mr. Tompkins also stressed the importance of understanding that it might be cheaper to "clean up" than to have a strong security program. His emphasis was on assessing and accepting risk because no matter how much is known of the past, managers must deal with the future. Mr. Tompkins stated that risk reduction analysis involves a complete economic analysis. Noting that the risk analyst should not be the decision-maker, he said that a quantitative assessment of risk is a reasonable approach for getting close enough because no absolutes exist in dealing with future events.

Mr. Tompkins also asserted that threat cannot be measured because it is the potential for harm. Noting the need to differentiate between vulnerabilities and threats, Dr. Marshall Abrams, Mitre, mentioned that at least one new vulnerability is identified each year. Dr. Abrams also commented that one way to assess risk is whether an agency might make the front page of the *Washington Post* newspaper.

2.8 Cryptographic Algorithm Metrics

Mr. Landgrave Smith, Institute of Defense Analysis, reviewed the metrics used for determining the strength of cryptography. Mr. Smith described pilot activities by a small working group to investigate the practicality of developing such metrics. The group selected a small sample of symmetric cipher block encryption algorithms in the codebook mode for confidentiality and an asymmetric public key algorithm. The group explored possible approaches to cryptographic metrics with a goal of encouraging the development of an American National Standard.

Although only a small sample of algorithms was analyzed, the focus of the pilot was essentially on speed of decipherment. A reasonably available, affordable platform was

chosen to perform the computations. The pilot defined five algorithm strengths: US-unconditionally secure, CS-computationally secure, CCS-conditionally computationally secure, W-weak, and VW-very weak. These designations were based on the length of time and amount of resource required to decipher the algorithms. For example, the US designation meant that plain text could not be determined from the cipher text regardless of how much resource was applied to decipherment and VW meant that the key could be determined systematically in 8 hours or so with about $20K effort. The results of the pilot demonstrated a set of possible metrics for cryptographic strength based on key length, attack time, steps, and rounds.

3. Panel Sessions

Two panel sessions were convened, one focused on case studies in Government and the other centered on industry. The intent of these panel sessions was to convey "real" experiences with defining and using metrics in managing IT security programs.

Panelists on the Government panel, moderated by Mr. Joe Leo, USDA, were: Ms. Jean Boltz, GAO; Mr. James Craft, U.S. Agency for International Development (USAID); Mr. Bill Hadesty, USDA; and Mr. Edward Keefe, U.S. Customs.

Panel members for industry were: Mr. Thomas Dunbar, Citigroup; Mr. Patrick Hymes, First Union Group; Mr. Robert George, Dupont; and Mr. Randy Sanovic, General Motors. The panel was moderated by Mr. John Sabo, Tivoli SecureWay.

3.1 Government Perspective on IT Security Metrics

Prior to remarks by panelists, the panel moderator, Mr. Joe Leo, USDA, made several observations. Calling security metrics more "an art than a science," he stated that Federal managers will be rated as if metrics are a science. The reality is that a significant use of metrics will be to make comparisons among programs. The challenge is to move from the old public service paradigm to the new twenty-four by seven paradigm while maintaining an appropriate security stance. Often the message is "just do it." Security is most often an after-thought. The issue of cost and funding cannot be ignored, either. Federal IT managers are faced with difficult choices and they may only be able to protect some applications -- those at greatest risk.

3.1.1 General Accounting Office (GAO)

In her comments, Ms. Jean Boltz pointed out that Congress is urging GAO to answer questions such as, "Is Federal computer security good enough?," "How do agencies security programs compare with each other?" and "Are agencies improving?" While all agencies are not audited every year, the GAO has been asked to perform more and more of these "grading" events.

Stating that "most agencies have serious weaknesses," Ms. Boltz summarized the current state of Federal computer security. She said that security controls selected and

purportedly implemented by agencies are often not effective. To improve, more precise measurements are needed.

Ms. Boltz indicated the GAO has had many internal discussions about how they would rank agencies. The prime consideration for GAO is how effective the security controls are, so GAO is focused on testing security controls. While no formal agreement has been reached on an "effectiveness" scale, initial thoughts are to assign a number based on a simple scheme comparable to other general audit findings (e.g., material weaknesses (level 1 and 2), reportable conditions (level 3), qualified (level 4), clean (level 5)).

So far, the findings are that, while improvements have been seen, the Federal community still has widespread and pervasive security problems. Several agencies are at the bottom of the ladder (level 1), meaning they have poor plans and weaknesses in every area audited. Other agencies demonstrate uneven security practices (level 2), with strong controls in some areas. Agencies labeled level 3 have generally effective security, with a few significant problems. Agencies exhibiting very effective security (level 4) do not have significant problems. Currently, only one agency, the Federal Reserve, has been identified as level 4. No agencies have achieved level 5 (i.e., a fully integrated security program).

Ms. Boltz emphasized the importance of understanding risk. Once controls to address the risk have been decided, they need to be tested. The GAO sees lots of examples where firewalls are misconfigured and not even turned on. Finally, some analysis of the benefit of the security controls needs to be done.

Summarizing the GAO effort, Ms. Boltz announced that the GAO staff has grown to 25-30 people and now includes a computer security testing lab. The scale for ranking agencies will continue to be refined. One goal is to enable comparisons across years to determine improvement.

3.1.2 U.S. Agency for International Development (USAID)

Affirming that metrics are used for many reasons, Mr. James Craft said that "measurement that isn't actionable is no good." The USAID has found that "micro-metrics" did not work, while "macro-metrics" has worked well in their situation. He described a scientific and management tool USAID has developed to measure success from the ground up.

Mr. Craft summarized his recipe for developing metrics by suggesting the following actions:

1. Prioritize what needs to be measured by determining how to get an action.
2. Take "baby steps" – do something "cheap, cheesy, and easy."
3. Use and repackage existing metrics.
4. Pilot.
5. Use evaluation software to show management.
6. Invest.

Mr. Craft also pointed out that USAID is two years ahead of schedule in closing the material weaknesses that were identified in the agency review. This is evidence that the USAID approach works.

3.1.3 Internal Revenue Service (IRS)

Mr. William Hadesty, currently with the U.S. Department of Agriculture, described his experiences at the IRS where he significantly improved the state of IT security. At the IRS, Hadesty used a risk-based approach coupled with audit techniques (based on his prior experience as a member of the GAO security team) to establish a baseline. He performed internal reviews looking at the condition (e.g., a particular problem), basing expectations on specified criteria, and identifying the cause and effect. These were inputs for action plans for improvement. He met to discuss workable solutions and timeframes with those most affected.

The IRS made a commitment of dollars, skills, and management to improving security. Hadesty's program employed about 90 experts in various IRM disciplines, 50 of whom were security-focused, who teamed to perform security reviews of IRS systems. Facilities were visited on a yearly basis, using audit method and tools to determine a baseline. Additionally, he was able to tie 30% of each manager's performance plan to how well they addressed security issues.

Another key component of Hadesty's campaign at the IRS was "awareness." For example, stressing that everyone has a role in security, he described social engineering incidents where lab technicians did not challenge "suits" (e.g., a well-dressed, official-looking individual) when they entered the laboratory. He raised security awareness by informing IRS employees that each and everyone of them should feel empowered to challenge a suit.

Hadesty also cautioned workshop participants to "make metrics valuable." Agencies have to conduct mission business and security will be the first to go if it is not relevant. Security must be thought of as "value-added."

3.1.4 U.S. Customs

Mr. Edward Keefe stated that Customs has put into place a process and procedure that will lead to a security metric. The Customs agency uses a star topology, contains a lot of legacy systems, and conducts sensitive law enforcement activities. They have developed an "Interconnection Security Agreement (ISA)" that, when combined with a Memorandum of Understanding (MOU), will instill security discipline in an organization. The ISA formalizes the interconnection arrangements between Customs and other non-Customs organizations.

More flexible than the legalistic MOU, the ISA specifies the technical requirements, (including any security constraints) among cooperating, communicating organizations.

The ISA identifies the systems being interconnected and describes the requirements and benefits of interconnection. The security features of the ISA are documented to protect the confidentiality, integrity, and availability of the data and the systems being interconnected. A topological diagram depicts interconnectivity from end-point to end-point. Also covered are "trusted behavior expectations," for example, that each system is expected to protect the information belonging to the other through the implementation of a security program that provides for defense against intrusions, tampering, viruses, and so on. Note that these are expectations and not guarantees. Incident reporting and audit trail responsibilities are also included in the ISA.

The ISA will be contributed to the "best security practices" website (see bsp.cio.gov) of the CIO Council's Security Privacy and Critical Infrastructure Protection Committee.

3.1.5 Discussion

Ms. Karen Worstell, AtomicTangerine and CSSPAB member, distilled two themes from the panel presentations. First, she identified a disconnect when trying to "sell" security. Should it be sold as loss avoidance or business enablement? The second point relates to operational context – why would we do metrics in the first place?

In response to the comment on operational context, Ms. Boltz pointed out that many agencies have not decided what is important and critical to protect, what risk is associated with lack of protection, and so they cannot figure out how much protection to apply. In fact, she said that sometimes GAO has to help agencies establish their risk concerns. Mr. Hadesty concurred, noting that agencies do not understand the value of the assets entrusted to them. Questions need to be asked about what are assets and what do they mean to the organization.

Mr. Knauf noted that more sharing across government is needed. He asked how can CSSPAB encourage more of this kind of exchange among agencies. Mr. Craft urged CSSPAB to endorse and foster the CIO Council's "best practices" initiative.

In a discussion of resources, it was pointed out that metrics can be used to define the dimension of the problem; however, a chicken and egg situation exists. Often resources are not applied until the problem is identified. Acknowledging that the improvements at the IRS were motivated by external forces (i.e., GAO report), Mr. Hadesty said the goal is to justify resources by the value-added of the activity and to identify shortcomings that cannot be addressed due to lack of resources. Essentially supporting GAO reviews, he said many problems can be solved inexpensively if they are known. They take attention and technical expertise but not a lot of dollars.

Ms. Michelle Moldenhauer, U.S. Department of the Treasury and CSSPAB member, stated that the Critical Infrastructure Assurance Office (CIAO) may have identified some metrics while looking at issues covering the impact of Federal agencies and the public. She suggested the Board invite a presentation on CIAO security metrics activities.

3.2 Industry Experiences with IT Security Measures

Moderator, Mr. John Sabo, Tivoli SecureWay, introduced industry panel members. Mr. Sabo described the synergy between the work of the private sector in the area of security metrics and the government, calling it unprecedented. He emphasized the importance of public-private partnerships in accomplishing commonly beneficial goals.

3.2.1 Citigroup

Mr. Thomas Dunbar summarized the activities of Citigroup's Corporate Information Security Office (CISO). The CISO is responsible for the non-technical aspects of information security in the corporation. Mr. Dunbar's focus is on awareness, training and educational programs, and metrics. The CISO program covers prevention, detection and verification, with metrics falling under the verification arm of the program.

The Citigroup's approach to metrics is that they be meaningful to the target audience, be easy to collect and interpret, be measurements to continuously improve security, be a yardstick to prioritize corrective action plans, and be a tool to assess the effectiveness of security offices throughout the corporation.

The Citigroup has developed an information security evaluation model. The model is comprised of five levels:

1. complacency,
2. acknowledgment,
3. integration,
4. common practice, and
5. continuous improvement.

Each level contains certain characteristics leading to results. Mr. Dunbar pointed out that Citigroup is working with the Federal CIO Council on their IT Security Assessment Framework (see section 2.4 of this report). Plans are underway to pilot the model in a Federal agency to see whether it will work in government as in industry.

Mr. Ronald Knode, Computer Science Corporation, suggested that whatever questionnaire (Framework) is used, the questions should be business-neutral. He said that organization is the key to choosing appropriate metrics.

3.2.3 First Union Group

Mr. Patrick Hymes described First Union's system security compliance monitoring program. Compliance is monitored against corporate information security standards, policies, and guidelines. The standards support the policies and define what controls are needed. The guidelines describe how to implement controls on a particular platform. The challenge is to ascertain whether or not people are following standards. Monitoring compliance helps satisfy concerns that risk is being addressed.

Thousands of systems encompassing multiple IT departments, low security awareness, technology evolution and complexity, time-to-market pressures, and immature and proprietary controls are some of the issues facing First Union. Compliance tools were developed and have been deployed on over 1200 systems, generating a monthly report to IT management. Compliance scores have improved and security awareness has increased. Mr. Hymes showed a sample monthly compliance report. In First Union, the key components to improved system security have been platform security guidelines, security education, consulting assistance, and compliance monitoring and enforcement.

Ms. Worstell pointed out that where security makes the business possible these factors should be highlighted as value-added. Likewise, if there are business actions that cannot be taken due to lack of security, these should be a part of the case for security, both in the private sector and in Federal environments.

3.2.2 Dupont

Representing the fibers and chemical industry, Mr. Robert George announced that "Dupont is the safest company in the world," placing a lot of value on safety. For Dupont, he said, information security is equivalent to safety. Stressing the strong ties between information security and safety, Mr. George called information security "the rules and regulations that safeguard the value-adding processes and the people whose skills develop, deploy and manage it." He prefaced his presentation by stressing the value of information, stating that "the only thing worse than the wrong people getting access to our information is not enabling access for the right people."

Mr. George described the DISO University and its activities. The DISO, Dupont Information Security Organization, is a web-accessible set of courses to educate security practitioners. It contains all levels of courses for accreditation and advancement.

He indicated that just as Dupont manages safety performance by metrics, it also manages information security by metrics. Dupont is developing a balanced score card of information security metrics, benchmarked with the best-in-class companies. The scorecard includes objectives, measures, benchmarks, and targets that promote change across four perspectives: financial, customer, internal, and learning.

Mr. George stressed that Dupont performs asset protection based on risk and on the Six Sigma management process. Six Sigma literally means 3.4 defects per million occurrences. A typical Six Sigma project for information security is password and user name management. Six Sigma measures the capability of the process to perform defect-free work. A defect is anything that results in failure.

At Dupont, information security is a priority. Annually a state-of-information-security letter is sent to Dupont's CIO, senior management, IT partners and the audit committee recapping security incidents, reporting information losses, estimating dollar loss by incident and category, indicating expenditures for information security, and giving a report card comparing Dupont with similarly situated companies.

3.2.4 General Motors

Mr. Randy Sanovic described the current state in General Motors (GM) where essentially the business model is changing. He said five tiers of dealerships exist and security passes through all of these. Policy exists along with authorized user procedures, standards for firewalls, and so on. A board audit committee addresses IT and security audits.

While hundreds of sample metrics are in place, not all are standardized. Some tailoring is done; however, overall, GM takes an enterprise view of metrics. Policy is reviewed, processes are analyzed, and checklists were developed for reviewing progress. A process for quality assurance and a process for risk management has resulted in GM's development of operations-based metrics.

3.2.5 Discussion

Mr. Sabo's question to the panel, "what's next for CSSPAB as far as security metrics are concerned?" prompted lively discussion.

Mr. Sanovic suggested that the starting point should be operating systems and applications. Mr. Dunbar said that laptop security is a major issue for Citigroup. Mr. Hymes pointed out that it is not clear who in government is in control of these issues, so he suggested that CSSPAB establish a role in metrics.

Mr. George recommended that the Board assess the idea of using standardized audits to evaluate security, indicating his belief that they are a robust way of looking at the overall processes. His opinion is that the Y2K experience left lots of Federal managers with information about what is in place. Suggesting an annual status of government computer security, Mr. George said he likes the idea of summarizing how each agency is doing. A standard way of comparing agencies would be a "good thing." Mr. George supports the notion of sharing sound practices and he stressed that agencies must know and understand risks.

Mr. Guida commented that rather than focusing on metrics from a tiered perspective, the concentration point should be management responsibility because agency missions differ. Mr. Reeder concurred, stating that "having a boss who cares" ultimately determines how much emphasis and resources are placed on security concerns.

4. Future Metric Activities

At the outset of the workshop, Dr. Abrams suggested that perhaps the most helpful output from the workshop would be a baseline or a common starting point. He pointed out the need to avoid "reinventing the wheel." While the initial intent was to "map the environment," perhaps the most useful result was the set of questions that need to be asked and answered.

The questions that evolved from the workshop fall into two categories – one related to security metrics specifically and one related to an appropriate role for CSSPAB with regard to security metrics.

With regard to metrics, questions were:

- What are metrics?
  - Metrics are different from measurements.
  - Metrics are a way of demonstrating to management the dimension of the problem.
  - Metrics are not statistics – need correlation point to measure effectiveness.
- Sometimes we measure what we can measure. Is that such a bad thing?
- Can we move from subjective to empirically-based objective measures?
- How can something that keeps moving be measured?
- Is a new paradigm needed, i.e., metrics not merely for systems and networks, but metrics for enclaves and perimeters – enterprise-wide security management?
- How good is IT security? Something simple but effective is needed that tells the story.

Mr. Frank Reeder, CSSPAB Chairman, pointed out that the intent of the workshop was to frame the discussion of what to do next. With regard to CSSPAB's role, the questions were:

- Can CSSPAB make a difference?
- How can CSSPAB be a catalyst?
- What leverage can CSSPAB bring to help resolve/add to the metrics issue?
- To what extent is the work of the Federal Government under the leadership of the CIO Council consistent with what the Board is hearing about the development of metrics?

5. Reflections

Many are taking the first steps to helping Federal agencies and industry deal with the complexity of protecting IT resources. The ability to measure the current state of effectiveness is crucial to continued and improved protection. Several cornerstone concerns resurfaced during the workshop:

- The need for more and continued interaction and sharing between and across civilian agencies and the national security community.
- The need for increased awareness and attention to computer security.
- The need for a common vocabulary, a common basis for communication.
- The need for increased resources to address security concerns.
- The need for more personnel skilled in security technology and techniques.

As Mr. Reeder summarized, this initial workshop performed "an environmental scan." Now is the time to determine what future actions the Board and others might take to further the state-of-the-art of measuring the effectiveness of security programs.

Appendices (available on the CSSPAB website: csrc.nist.gov/csspab/)

1. November 1998 letter from Raymond Kammer, NIST Director, to CSSPAB
2. "Security Metrics – What Are They" – Stuart Katzke, National Security Agency
3. "Defense Information Assurance Program (DIAP) – Information Assurance Readiness Assessment Metrics – Terry Bartlett, DIAP/DOD
4. "Systems Security Engineering Capability Maturity Model (SSE-CMM) Profiles, Assurance and Metrics (PAM) Working Group – George Jelen, ISSEA
5. "Information Technology Security Assessment Framework" – John Gilligan, U.S. Department of Energy
6. "Information Security Metrics – An Audit-Based Approach" – Jennifer Bayuk, Bears, Stearns, & Co.
7. "Overview of FISCAM – Chapter 3" – Darrell Heim, GAO
8. "Quantitative Risk Assessment" – Fred Tompkins, Key Technologies & Security Inc.
9. "Cryptographic Algorithm Metrics" – Landgrave Smith, Institute for Defense Analysis
10. Government Panelists Handouts – Jean Boltz, GAO; James Craft, USAID; Edward Keefe, U.S. Customs
11. Industry Panelists Handouts – Thomas Dunbar, Citigroup; Patrick Hymes, First Union Group; Robert George, Dupont

Attendees (alphabetical by organization represented)

Frederick Weingarten, American Library Association (CSSPAB member)
Karen Ferraiolo, Arca Systems, Inc.
Karen Worstell, AtomicTangerine (CSSPAB member)
Jennifer Bayuk, Bear, Stearns and Co. (Speaker)
Natalie Givans, Booz, Allen
Thomas Dunbar, Citcorp (panelist)
Ronald Knode, Computer Science Corporation
Clay Wilson, Congressional Research Service
Terry Bartlett, Defense Information Assurance Program (Speaker)
Grace Culver, Defense Security Services
Robert George, Dupont (Panelist)
William Gill, Environmental Protection Agency
Diane Frank, Federal Computer Week (Press)
Trina Dinavo, Federal Sources
Peter Browne, First Union Corporation (CSSPAB member)
Patrick Hymes, First Union Corporation (Panelist)
Sharon Damon, General Accounting Office
Darrell Heim, General Accounting Office (Speaker)
Jean Boltz, General Accounting Office (Panelist)
Randolph Sanovic, General Motors Corporation (Panelist)
James Tippett, Independent Consultant
Ann Brown, Indian Health Service
Landgrave Smith, Institute for Defense Analysis (Speaker)
George Jelen, International Systems Security Engineering Association (Speaker)
George Trubow, The John Marshall Law School (CSSPAB member)
Fred Tompkins, Key Technologies and Security, Inc. (Speaker)
Stephen Lipner, Microsoft Corporation (CSSPAB member)
Marshall Abrams, The Mitre Corporation
Robin Medlock, Mitretek Systems
Elaine Frye, National Institute of Standards and Technology (CSSPAB Secretariat)
William Mehuron, National Institute of Standards and Technology
Susan Zevin, National Institute of Standards and Technology
Fran Nielsen, National Institute of Standards and Technology (Workshop Coordinator)
Edward Roback, National Institute of Standards and Technology (CSSPAB Secretariat)
Marianne Swanson, National Institute of Standards and Technology
Daniel Knauf, National Security Agency (CSSPAB member)
Ed Steeble, National Security Agency
Stu Katzke, National Security Agency (Speaker)
Craig Sherman, Office of Federal Housing Enterprise Oversight
Kamela White, Office of Management and Budget
Franklin Reeder, The Reeder Group (CSSPAB Chairman)
Lynn McNulty, RSA Security
John Sabo, Tivoli SecureWay (CSSPAB member, Panel moderator)

James Craft, U.S. Agency for International Development (Panelist)
Edward Keefe, U.S. Customs Service
Bill Hadesty, U.S. Department of Agriculture (Panelist)
Joseph Leo, U.S. Department of Agriculture (CSSPAB member, Panel moderator)
Sue Weis, U.S. Department of Agriculture
Robert Kling, U.S. Department of Agriculture, NRCS
Linda Laboski, U.S. Department of Commerce
Nancy Majower, U.S. Department of Commerce, NOAA
John Gilligan, U.S. Department of Energy (Speaker)
Peter Salatti, U.S. Department of Energy
Bernardene Walford, U.S. Department of Labor
Emory Anderson, U.S. Department of the Navy
Patricia Black, U.S. Department of the Treasury
Richard Guida, U.S. Department of the Treasury (CSSPAB member)
Michelle Moldenhauer, U.S. Department of the Treasury (CSSPAB member)
James Wade, Verizon Wireless (CSSPAB member)