U. S. Government Use of the Systems Security Engineering Capability Maturity Model (SSE-CMM)

Panelists:
Mr. James P. Craft, United States Agency for International Development
Charles G. Menk III, National Security Agency
Panel Chair:
Mary D. Schanken, National Security Agency

Panel Abstract

The current ways that commercial security products and services come to market are inadequate. Products and systems either go through a lengthy and expensive evaluation process, which result in a product or a system that no longer meets current needs, or they go through little or no external evaluation, leaving the buyer to trust the providers' claims. Further, services are all marketed on this caveat emptor basis (buyer beware.)

The National Security Agency (NSA) has been involved in efforts to help customers judge the full spectrum of Information Systems Security (INFOSEC) products, systems, and services while possibly minimizing the expense and time involved in the current evaluation/certification processes. An effort that NSA sponsored was the development of a Capability Maturity Model (CMM) for security engineering.

NSA began the effort to develop a CMM for security engineering in 1993, with the hopes that the security engineering community would become involved to help define the criteria against which they might be assessed in the future. Learning from the past, NSA believed this approach would be more successful and accepted than if NSA were to issue it as a requirement. Over 50 government, industry, and academic organizations developed the Systems Security Engineering Capability Maturity Model (SSE-CMM) and its appraisal methodology. This panel will address a few of the ways that the United States Government is using the SSE-CMM.

Mary D. Schanken, National Security Agency
schanken@romulus.ncsc.mil

Ms. Mary Schanken leads the Developmental Assurances Team for the National Security Agency (NSA). As an Information Systems Security expert, her specialty is developing alternative methods of assurance for producing products, systems, and services that maintain and protect information. She is working to address the area of Standards and Best Practices as outlined in Presidential Decision Directive 63, which calls for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. She was a key contributor in the development of the Trusted Computer System Evaluation Criteria Rainbow Series, the Federal Criteria and the international Common Criteria. Ms. Schanken began her Information System Security career as a Trusted product Evaluator. She previously held the position as the first Chief of the NSA Information Systems Security Organization Service Center. She

was a member of the international Common Criteria Assurance Approaches Working Group, which examined how five alternative assurance methods mapped to the Common Criteria. She served as the government lead for the Systems Security Engineering Capability Maturity Model (SSE-CMM), which is the product of a voluntary collaboration of 50 government and commercial organizations to meet the needs of the security engineering community. She participated in pilot appraisals to validate the SSE-CMM and its appraisal methodology. Recently, her focus as turned to implementing the SSE-CMM within the Department of Defense. Ms. Schanken is a Lead Assessor for the National Voluntary Laboratory Assessment Program (NVLAP) where she assesses a laboratory's ability to perform evaluations using the Common Criteria. She completed her Computer Science degree from the University of Maryland Baltimore County, and graduate work in Computer Systems Management from the University of Maryland University College. In addition to her full time responsibilities, she is enrolled in the Naval War College non-resident program.

Mr. James P. Craft, United States Agency for International Development
jcraft@usaid.gov

Mr. James P. Craft is the Information Systems Security Officer and Information Systems Security Program Manager for the United States Agency for International Development. In this capacity, Mr. Craft has led the development of the Model Information Systems Security Program (MISSP).

Mr. Craft has more than nineteen years of experience in the areas of systems and security engineering; operations and strategic planning; telecommunications; Test, Training, and Exercise (TT&E); organizational analysis; and management. This experience has, for the last fifteen years, primarily centered on systems engineering, information security, and operations in large MIS/EIS systems with specialized applications operating across multimedia LAN/WANs. Mr. Craft served as a communications officer in the United States Marine Corps, and worked for the firms of BETAC, Booz-Allen & Hamilton, and Systems Research and Applications International prior to his appointment to USAID. Mr. Craft has served on the Steering Committee, Author Group, and Applications Group for the SSE-CMM. Mr. Craft also assisted the Presidential Commission on Critical Infrastructure Protection in developing a comprehensive summary of threats and impacts to the national and global information infrastructure.

Mr. Craft is a speaker and published writer who has written issue papers, policy papers, technical papers, SOPs, studies, manuals, and other analysis. As a government contractor, Mr. Craft has worked with and supported Information Technology and security programs of the NSC, NSA, NCS, DOD, DOJ, FBI, USSS, Department of State, GSA, NIST, DOE, Department of Treasury, and other Federal organizations. Mr. Craft has also supported private organizations including law firms, banks, stock exchanges, energy and other firms.

Mr. Craft received a B.S., Management from George Mason University in 1978.

Mr. Craft is a Certified Information Systems Security Professional as determined by the International Information Systems Security Certification Consortium.

Topic Abstract

The United States Agency for International Development (USAID) is in the midst of an effort to develop and validate a Model Information System Security Program (MISSP).

The Government Accounting Office has highlighted material computer security weaknesses in all Departments and Agencies that they have examined. For its part USAID has begun building a best practice based system security program from the ground up.

The model program presented herein has grown out of an initial program response to unsatisfactory audit reports from USAID Office of Inspector General. However, as USAID has continued to establish a complete life-cycle ISS program, it discovered that our the program would be improved, and other agencies could benefit, if USAID expanded this effort to serve as a model program incorporating ISS best practices from government.

The approach taken by USAID was to merge together national guidance, existing security initiatives, and functional and process models such as the Systems Security Engineering Capability Maturity Model (SSE-CMM) to create program frameworks that should be applicable to other Federal organizations. USAID is now identifying and integrating best practices and Commercial Off the Shelf (COTS) tools for portions of the MISSP, which will be the focus of the MISSP. The MISSP draws heavily from the SSE-CMM and seeks to use it as a process model. Many of the requirements for specific best practices grew out of the SSE-CMM.

Mr. Craft's presentation will discuss the progress that USAID has had in applying the SSE-CMM to its own program and this exciting Federal initiative.

Charles G. Menk III, National Security Agency
menk@constitution.mil

Graduate Marquette University with Bachelors of Science Computer Science in 1987
Graduate Loyola College of MD with Masters of Engineering Science (CS) in 1995
Served as US Naval Officer from 1987-1993
Served as Computer Systems Evaluator from 1990-1996
Served as Lead System Security Engineer on SSE-CMM development effort, 1996-1999
Member of the SSE-CMM Author Group, and Appraisal Methodology Working Group
Co-author of INFOSEC Assessment CMM
Co-author of SSE Business CMM
Co-author of NVLAP CMM
Participated in over 8 CMM appraisals as Facilitator and Team Leader
Trained ISSO 9000 Lead Auditor

Topic Abstract

In April, 1999 version 2.0 of the SSE-CMMM and Appraisal Method were released thus closing the book on the development effort. The program has now shifted into an implementation activity.

The SSE-CMM was developed to be a versatile tool. As such, there are currently multiple initiatives in use today based on the SSE-CMM effort. One initiative is the NIST/NSA backed INFOSEC Assessment program. Another is the NIST/NSA backed NVLAP version as well as an internal NSA SSE-Business version of the model. While these three initiatives have taken great liberties in their tailoring of the SSE-CMM, their efforts would not have been as effective without the underlying work and procedures supplied by the SSE actions in previous years.

As the world continues to be thrown into more and more high tech applications and development activities, the need for clear and concise procedures will become paramount to success. Success in terms of on-time and under budget and repeatable results. The need for having DETERMINISTIC measures, to assess a company's ability to deliver what the say they can within the rates expected, is fast becoming a major focus for large contracts throughout the DoD, US Government and industry alike. The SSE-CMM provides a metric that can be used to mitigate these concerns as well as the added benefit of a layer of security normally overlooked in today's fast paced, "get-it-to-market-now" approach.