INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

JUL 30 2008

The Honorable Jim Nussle
Director
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Nussle:

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

On numerous occasions over the past several years, the Board has heard briefings and held discussions around the issue of whether metrics developed under FISMA to assess Government security have, in fact, focused attention in a way that improves agency understanding and performance in this critically important area. At the same time, the Board has also examined the efficacy of security metrics more generally, and the extent to which such metrics can serve as indicators of security progress and performance.

As a result of these inquiries, the Board has found that the FISMA metrics program served a salutary role in enhancing focus on agency security activities. The metrics program, as implemented by OMB policy and NIST guidance, has led to:

- Increased attention throughout the government on the importance of good process;
- Better documentation of security programs and plans;
- Improvements in third-party reviews, especially from the Inspector General community; and
- Stronger engagement by senior management in security activities

The record set before the Board, however, points to a less positive yet highly significant finding as well. Considerable evidence demonstrates that FISMA implementation has become overly compliance-driven, with excessive attention to the fulfilling Certification & Accreditation (C&A) and other reporting processes at the expense of implementing, measuring, and improving true security performance. Agency senior executives, CIOs, CISOs, and even Inspectors General have all indicated that voluminous documentation requirements have gone too far, leading to a check-the-box set of activities that reward compliance rather than outcomes. Private sector experts have echoed and amplified this view. Agencies often write or contract for security documentation after the fact, rather than embedding and documenting security during development to insure that security is built into programs and systems up front – an industry best practice.

The Board has identified examples of worthwhile metrics within the FISMA framework, including traditional perimeter measures like intrusion detection, penetration testing, and incident response. But even when they have been obtained, such results are lost amidst the need to comply with the much larger set of FISMA-related procedural requirements; as a result, agencies lack time and resources to develop and implement needed improvements in their security program. While a comprehensive documentation assessment approach may have had value in setting the FISMA baseline (i.e., during the first several reporting cycles), the Board believes that the benefit of measuring detailed processes has become far outweighed by the burden this places on agencies, and the opportunity cost of resources devoted to compliance rather than performance.

Accordingly, the Board recommends that FISMA and related policy and guidance be revised so that agency and contract incentives are to measure and improving actual security. We recognize that perfect security, as well as perfect security measurement, is an aspiration rather than an attainable state; indeed, the Board has heard important briefings about the limits of security measurement, and does not suggest that a sound metrics program will address all potential vulnerabilities or enable a sound response to all threats. However, an explicit, outcome-based set of metrics would make agency security performance more transparent, would point to a concrete set of actions related to improvement over time, and would increase underlying trustworthiness of and with agency IT systems. These metrics should focus on risk management, rather than compliance; should have a line of sight to business and program goals, rather than IT operations; and should assess both status and progress.

The Board holds that an improved FISMA metrics program would address management, operational, and technical controls, as outlined under current OMB policy and NIST guidance, but would neither measure nor reward process documentation. As a result, agencies could spend more time and resources understanding their actual security posture, and taking steps to improve. To accomplish this, we recommend that OMB and NIST work with agency CIOs to review FISMA policy and guidance, and eliminate all provisions not necessary to measure and improve security in a way that manages risk and improves program delivery. Metrics to eliminate might

include percent of systems C&Aed, as most systems have gone through this baseline; number of training sessions conducted, since much of this training is superficial at best; and duplication of measures between the CIO and IG.

The Board also recommends that the metrics required under a new FISMA program be issued by OMB guidance as early as possible in the fiscal year for which reports are made, rather than late in the year as has often been the case given the many competing demands of the IT calendar. The security of Federal systems has become a mission critical element in assuring good program performance; measuring the way that security enables or hinders that performance should be a systematic and continuous activity, rather than one that comes late in the year and is thus largely divorced from ongoing program operations. On a longer term basis, a revised FISMA process could mandate that OMB, NIST, and the CIOs could periodically review metrics (e.g., every 2 years), with an eye towards updating them based on perceived success. This process would create an institutional imperative for FISMA to stay current, and promote positive adaptation in a world where attacks change, defenses change, and baseline systems improve.

The Board further recommends that the OMB use its procurement policy authority to amend the Federal Acquisition Regulation (FAR), so that agency contract documents (e.g., RFPs, RFQs, contract compliance reports) incentivize industry to build and measure security based on the same outcome-oriented metrics that are issued in OMB policy and NIST guidance – and so that these documents do not require unrelated security activities that add cost and burden to the acquisition system with little or no return. The Administration has made some progress on policy in this area, and has developed related FAR clauses. However, implementation is sketchy at best; the Board's industry members echo comments we have heard from industry briefers, who contend that contracted security resources would be far better able to solve real problems if contract requirements focused on substantive rather than procedural security activities.

The Board has also heard from NIST officials about their long-term research efforts on security metrics. We commend NIST for undertaking this effort, though we have questions about its applicability to agency security programs given its emphasis on mathematical modeling. We believe that continued actions to link metrics R&D with law, policy and guidance will make the benefits of NIST activities more applicable to agency program improvement. We recommend that OMB and NIST work with interested stakeholders, including CIOs, CISOs, IGs, program officials, and private sector experts, to review and enhance the metrics program over time.

Finally, the Board recommends that FISMA policy and guidance encourage accountability for security program performance, through rewards for progress and the maintenance of strong outcomes, and consequences for deterioration and continued weak outcomes. Improving security in agencies requires more than a good set of metrics. Managing this change will need to address behaviors and the political, career executive, program management, and operational levels.

We appreciate the opportunity to offer the Board's views on this critically important issue. Please let me know if the Board can answer any questions or take additional actions to support improvements in Federal information security metrics.

Sincerely,

Daniel J. Chenok
Information Security and Privacy Advisory Board Chairman

cc: Karen Evans