SAFEGUARDING AGAINST OUTSIDE AND INSIDE THREATS THROUGH REAL TIME CONTINUOUS MONITORING

In the Matter of	)	
	)	
NIST Special Publication 800-137	)	Initial Public Draft
Information Security Continuous	)	
Monitoring for Federal Information	)	
Systems and Organizations	)	
	)	

March 2011

Comments of
The Center for Regulatory Effectiveness
1601 Connecticut Avenue, NW
Washington, DC 20009
202.265.2383
www.TheCRE.com

SAFEGUARDING AGAINST OUTSIDE AND INSIDE THREATS THROUGH REAL TIME CONTINUOUS MONITORING

In these comments, the Center for Regulatory (CRE) will emphasize three key points in addition to the other valuable recommendations that are being provided to NIST on enhancing the utility and other quality aspects of Special Publication 800-137. CRE's three primary recommendations are:

1. Transparency. NIST needs to speedily make public all comments received on the draft document. CRE will also discuss the role of our FISMA Focus Interactive Public Docket (http://www.thecre.com/fisma/) in supporting a substantive, transparent discussion of continuous monitoring issues.

2. Substantial Equivalence. NIST should include a "substantial equivalence" provision in the guidance document to enhance compliance flexibility while maintaining rigorous monitoring requirements.

3. More Exacting Definition of Continuous Monitoring. The definition of continuous monitoring underlies the entire guidance document and, thus, the final component of NIST's Risk Management Framework.[1] NIST needs to put some meat on the bones of its current definition of continuous monitoring.

I. The Transparency Imperative – Making Public Comments Public

FISMA compliance is becoming less and less of an internal-only federal issue. Instead, FISMA-related documents are increasingly applicable to the private sector. NIST recognized the private sector applicability of federal information security documents in their draft Interagency Report 7756, "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture," which stated that the document was "designed to be applicable to industry, state governments, and tribal networks through using a flexible architecture able to handle diverse customers and uses."

In addition to any voluntary industry compliance with FISMA requirements, legislation has been introduced in the House which would authorize federal officials to "establish and enforce risk-based cybersecurity requirements for private sector computer networks within covered critical infrastructures."[2]

---

[1] http://csrc.nist.gov/groups/SMA/fisma/framework.html.

[2] H. R. 174, Homeland Security Cyber and Physical Infrastructure Protection Act of 2011.

The Cybersecurity and Internet Freedom Act of 2011, introduced in the Senate, contains numerous provisions related to continuous monitoring. With respect to the private sector, the legislation would require that federal officials "with responsibility for covered critical infrastructure...in consultation with...any private sector entity determined appropriate by the Director, shall, on a continuous and sector-by-sector basis, identify and evaluate the cyber risks to covered critical infrastructure."

Applicability of FISMA requirements to the private sector heightens the need for transparent development of the standards and guidance. Even if the FISMA documents were purely for internal federal use, a fully transparent development process should be used in order to enhance the quality of the publications. America's cybersecurity defense requirements are too important to be left to a cloistered process.

NIST has taken a major step toward transparency by engaging in the public comment process on draft documents. CRE applauds NIST's decision to accept public comment and requests that they take an additional crucial transparency step by making public all comments received by the agency.

Two key benefits of making comments public are:

1. Vetting of comments received. By making comments on the public draft public, NIST would allow – and benefit from – interested parties being able to analyze, comment on, support and/or criticize the ideas, assertions and other materials presented in the comments.

2. Transparency of agency response to comments. By allowing the public to see the comments of the regulated community and other interested parties, NIST would allow stakeholders to understand how the various comments affected NIST's decisions on revising the draft document, a basic component of transparency.

CRE requests that NIST place our comments on an e-docket on their website or other publicly accessible forum. CRE further requests that NIST quickly make public all comments received from governmental and non-government entities in response to their request for comment on the Initial Public Draft of SP 800-137.

It is important to note that establishing public dockets of comments received on non-regulatory technical and scientific policy issues is standard operating procedure in the Obama Administration. For example, the following is a link to one of the e-dockets established by the White House on ocean policy, http://www.whitehouse.gov/administration/eop/ceq/initiatives/oceans/interim-framework/comments. We also note that NIST, along with its sister agencies, NTIA and ITA, established a public docket of comments received on an important non-regulatory cybersecurity policy issue, publishing the comments on the NIST website at http://www.nist.gov/itl/cybercomments.cfm.

CRE makes its request for NIST to release all comments on the Initial Public Draft pursuant to:

1. President Obama's Open Government Directive which, in addition to other transparency steps, requires agencies to "respect the presumption of openness by publishing information online.... Timely publication of information is an essential component of transparency."[3]

2. The Freedom of Information Act (FOIA). Accordingly, in addition to serving as CRE's comments on NIST Special Publication 800-137, these comments also constitute a request under the Freedom of Information Act, 5 U.S.C. Sec. 552, for all comments received by NIST on the draft publication SP 800-137. A copy of these comments and FOIA request is being provided to NIST's Freedom of Information Act Officer.[4]

FISMA Focus: An Interactive Public Docket

Interactive Public Dockets (IPDs) are described by Wikipedia as eRulemaking tools "created and managed by non governmental organizations that seek to provide the public with the capability to: 1) publicly post data and other materials pertaining to federal proceedings on a continuous basis, including after the close of the Administrative Procedure Act comment period; and 2) post comments on already submitted materials."[5]

CRE created FISMA Focus, found at http://www.thecre.com/fisma/, to promote informed discussion and enhance public participation "centered on federal cybersecurity policy compliance issues with a particular emphasis on Continuous Monitoring."[6] Continuous monitoring was chosen as the initial thrust of the forum due to its direct applicability to the private sector.

CRE will be posting comments on the continuous monitoring draft document on FISMA Focus' NIST SP 800-137 Discussion Forum found at http://www.thecre.com/cm/. All interested persons can use the forum to comment on the documents posted or to post their own documents. To ensure ease of use, no registration is required and comments may be posted with or without attribution at the poster's discretion. To encourage substantive discussion, users may post large files (up to 100 MB) in a variety of formats (PDF, MS Word, mp3, wmv, etc.) in support of their views.

All comments received on FISMA Focus, with exception of spam, obscenity and other clearly inappropriate material, will be posted following moderation.

---

[3] Found at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

[4] http://www.nist.gov/admin/foia/#sample.

[5] http://en.wikipedia.org/wiki/Interactive_Public_Docket.

[6] http://www.thecre.com/fisma/?page_id=2.

II. Substantial Equivalence

The continuous monitoring guidance document should include a discussion of "substantial equivalence." The concept of substantial equivalence was first developed by the Organisation of Economic Co-operation and Development (OECD) in the early 1990s "as being the most practical approach to addressing the safety of foods and food components derived through modern biotechnology...."[7] The OECD further explained that "[s]ubstantial equivalence is not a quantitative criterion or a hurdle, but a framework for thinking."[8]

The same framework that is the most practical approach to thinking about food safety is also essential when thinking about IT safety.

It should be noted that federal agencies ranging from the Food and Drug Administration (FDA) to the Department of Housing and Urban Development (HUD) have adopted the concept of substantial equivalence and applied it to various areas of compliance assurance. For example, HUD reviews applications from state or local housing agencies to determine whether they enforce "a law that provides substantive rights, procedures, remedies and judicial review provisions that are substantially equivalent to the federal Fair Housing Act" and, if so, provides them with a "substantial equivalence certification" that confers various benefits.[9]

Within the context of continuous monitoring and FISMA, substantial equivalence would mean that an organization has the option of implementing a continuous monitoring program that provides substantially equivalent security assurances as one that conforms with the SP 800-137 guidance. NIST, in consultation with OMB, would need to verify an agency's substantial equivalence assurance.

A substantial equivalence assurance process would be fully in keeping with FISMA which requires that NIST, in developing of standards and guidelines, "to the maximum extent practicable"

> *ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and*

---

[7] Organisation for Economic Co-operation and Development, "Series on the Safety of Novel Foods and Feeds No. 21: CONSENSUS DOCUMENT ON COMPOSITIONAL CONSIDERATIONS FOR NEW VARIETIES OF PAPAYA (Carica papaya L.): KEY FOOD AND FEED NUTRIENTS, ANTI NUTRIENTS, TOXICANTS AND ALLERGENS," 02-Jun-2010, p. 11.

[8] Organisation for Economic Co-operation and Development, "GM FOOD SAFETY: FACTS, UNCERTAINTIES, AND ASSESSMENT: The OECD Edinburgh Conference on the Scientific and Health Aspects of Genetically Modified Foods - 28 February - 1 March 2000, Chairman's Report," p. 3.

[9] http://www.hud.gov/offices/fheo/partners/FHAP/equivalency.cfm.

> *use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products.* 15 USC 278g-3 (c)(6)-(7) [Numbering omitted, emphasis added]

CRE recommends, therefore, that:

- Special Publication 800-137 clearly state that continuous monitoring methodologies and technologies, including off-the-shelf security products, which achieve substantial equivalence with the objectives set forth in the document are acceptable; and

- NIST, in cooperation with OMB, the regulated community and private sector stakeholders, develop a substantial equivalence verification program for continuous monitoring.

III. The Need for Specificity/Defining Continuous Monitoring

A. The Need for Specificity

One of the themes that runs through CRE's comments on the draft document is the need for greater specificity. For the guidance document to be a useful tool in improving cybersecurity, not simply serving as a *pro forma* guidance that can mean pretty much whatever a user wants it to mean, it needs to provide crisp, clear definitions and guidance.

B. Defining the Term "Continuous Monitoring"

The definition of "continuous monitoring" in Appendix B of the draft document lacks power and impact and yet it is the basis for much of the policy in the proposed NIST Guidance. CRE recommends replacing this term in the Glossary with one of the recommended definitions below. It would be beneficial to include the more substantive definition in the Executive Summary and a rewording of it in the introductory paragraphs of sections where the conceptual framework is elaborated, such as Chapters 2 and 3.

1. Enhancing the Definition of Continuous Monitoring

Current Definition of Continuous Monitoring: "Maintaining ongoing awareness to support organizational risk decisions, vulnerabilities, and threats to support organizational risk management decisions. See *Information Security Continuous Monitoring, Risk Monitoring* and *Status Monitoring.*"

Three Possible Enhanced Definitions for Continuous Monitoring. Instead of the vague current definition above which lacks utility to users, CRE recommends that NIST adopt one of the following three enhanced definitions of Continuous Monitoring.

- Enhanced Definition 1. An automated process by which actionable metrics are developed from a reasoned, thorough awareness of system processes and interactions. Continuous Monitoring captures intentional, unintentional, inadvertent/ancillary actions, irrespective of origin, that may increase the monitored system's vulnerability to a degradation of performance, the unauthorized acceptance, processing or transmission of data, or which may otherwise compromise the organizational mission of the system owner/operator. Reports generated by Continuous Monitoring are developed, formatted and provided to authorized persons/organizations to improve the quality of system risk-response decisions by role players within Tiers (1), (2), and/or and (3). Continuous Monitoring solutions must be able to detect patterns in real time against insider threats as well as externally generated hazards. The ability to understand different and handle large data volumes is critical.

- Enhanced Definition 2. A specific means for maintaining ongoing situational awareness of the monitored system's processes and interactions. Continuous Monitoring systems generate and report actionable decision metrics relevant to role players in Tiers (1), (2) and/or (3) at established frequency intervals based on risk tolerance by recording and analyzing intentional, unintentional, inadvertent/ancillary actions, irrespective of origin, that may increase the monitored system's vulnerability to a degradation of performance, the unauthorized acceptance, processing or transmission of data, or which may otherwise compromise the organizational mission of the system owner/operator. The ability to report on data quickly and provide *ad hoc* searching capabilities are necessary in order to meet compliance mandates such as Cyber Scope and frequency to advise of risk tolerance.

- Enhanced Definition 3. An ongoing observance and analysis taking place after the initial system accreditation which provides awareness of, warning as appropriate, and decision support regarding intentional, unintentional, inadvertent/ancillary actions, irrespective of origin, that may increase the monitored system's vulnerability to a degradation of performance, the unauthorized acceptance, processing or transmission of data, or which may otherwise compromise the organizational mission of the system owner/operator and which provides actionable decision metrics relevant to role players in tiers (1), (2) and/or (3). Continuous monitoring systems need real time alerting and the ability to detect patterns for complete situational awareness as well as forensics that occur after the fact.

2. Continuous Monitoring Knowledge Statement – A Component of the Definition

The definition of Continuous Monitoring selected/developed by NIST should include, as an integral component, the following statement from DHS' Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS), version 1.8, "Continuous monitoring of computing and network assets requires up-to-date knowledge

of the security posture of every workstation, server, and network device, including operating system, software, patches, vulnerabilities, and antivirus signatures."[10]

IV. Other Comments on SP 800-137

A. Overview

The continuous monitoring process figure on p. 20 was very helpful in communicating the concept of what goes into an ideal program. It seemed, however, that it was necessary to weed through some fluff before being able to identify what NIST actual stance and guidance as it relates to continuous monitoring.

The Executive Summary highlighted NIST's stance but focused on explaining why monitoring is important without making that immediate connection to why it is important to monitor continuously. NIST should set the appropriate tone early in the document. CRE recommends introducing the continuous monitoring process components (at a high level) up front in the Executive Summary then explain its interaction with various components of a security program.

The document needs to provide more concrete guidance on how organizations can effectively introduce and implement a robust continuous monitoring program to their environment.

B. Enhancing the Discussion of Frequency

The draft document's discussion of the importance and applicability of the frequency and assessment of monitoring is on point and thorough; however it misses an important opportunity for specificity and punch, and, above all, an increase in utility. Specifically, the discussion should add a time component that is further defined by Tiers (1), (2) and (3). Moreover, SP 800-137 must make clear that continuous monitoring means real-time monitoring. Allowing lags or gaps in monitoring coverage reduces security effectiveness by providing opportunities for harmful actions.

The document should include also include a discussion explaining the importance of automated and manual verification of the continuous monitoring measures. There is the need for one or more specific, named individuals to verify and attest that the continuous monitoring strategy is being implemented correctly, operating as intended, and meeting stated security objectives. The most sophisticated continuous monitoring tools will be useless, except for post-mortem purposes, if the knowledge gained is not dispensed on a timely basis to the person(s) with the authority and responsibility to address it.

- In order for a continuous monitoring to be effective, it needs to include a component requiring documented human awareness of relevant results.

---

[10] http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf.

CRE recommends assigning a specific time review function to the criteria identified on pages 29-30 as an example with an illustration by role or Tier. Time frequencies for human review and processing and acting/not acting decisions, can be defined in scenarios added as an illustration in Chapter 3 or in an appendix. All controls are important and must be monitored in some fashion but some controls are more important than others and need to be monitored at different levels and with different frequency. Defining the important level of each control will be vital for each respective agency in determining what monitoring frequencies are needed.

The role of Security Content Automation Protocol (SCAP) should be closely aligned with the frequency component as an emerging strategy for continuous certification and accreditation. Some of significant benefits of SCAP should be referenced as follows:

1. With near real-time continuous monitoring capability, SCAP would enable Continuous C&A to test controls significantly more often than may be required.

2. SCAP threat and situational analysis feeds would inform both the authorization and continuous monitoring process.

3. The information captured by SCAP continuous monitoring would inform the validation of Department information system security plans.

4. SCAP continuous monitoring would enable real-time risk decision making.

CRE recommend defining the steps and an individual's role/responsibilities for responding to a risk. This should be defined by an illustration in the appendix.

CRE also proposes adding a frequency monitoring definition to the glossary similar to what follows:

> ***Recommended Definition of Frequency Monitoring*:** Determined time frames (24/7, static schedule, monthly, weekly, annually, identified trigger, etc.) for verifying that the outputs from the continuous monitoring systems and protocols are delivering, to the appropriate person(s), accurate, relevant and useful knowledge for risk-related decision-making based on tier-specific metrics defined by mission clarity, volatility, impact of error/non-delivery, known weaknesses and vulnerabilities, risk tolerances and user defined or desired changes, within objectives, needs and budgets.

C. Cost Effectiveness: Moving Beyond Paper-Based Audits

NIST's continuous monitoring guidance document needs to play a key role in cybersecurity cost control. Specifically, continuous monitoring systems should include the capability of automated on demand/real-time reporting so as to allow organizations to demonstrate security control compliance without the need for "paper based" audits.

D. *Ad Hoc* Search Capability: A Core Continuous Monitoring Capability

One of the core capabilities that any effective continuous monitoring system needs to provide is the ability to analyze selected system data. In order for continuous monitoring tools to provide such analytic capabilities, they have to provide officials the ability to search for whatever monitored data points they choose. Thus, the guidance document needs to emphasize the importance of an ad hoc search capability as an integral capability of a continuous monitoring system.

E. Due Diligence/Due Care

The Executive Summary of the draft guidance document should include a discussion emphasizing the crucial roles of Due Diligence and Due Care.

A prudent person takes due care to ensure that everything necessary is done to operate the organization according to sound principles and in a legal, ethical manner. A prudent person is also diligent; *i.e.* mindful, attentive, and ongoing in their due care of the business. Such prudence is directly applicable to the continuous monitoring function. Specifically, a common unrecognized ethical dilemma exists when an IT auditor provides both continuous auditing and continuous monitoring: the potential for losing long-term auditor independence and objectivity because of the different purposes each service has within an organization.

The document should also add definitions of Due Diligence and Due Care to the Glossary similar to what follows:

> ***Recommended Definition of Due Diligence*:** Performing reasonable examination and research before committing to a course of action and continuing activities that make sure the protection mechanisms are continually maintained and operational.
>
> ***Recommended Definition of Due Care*:** The level of diligence which a prudent and competent person would exercise under a given set of circumstances. Due professional care applies to an individual who professes to exercise a special skill such as information system auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by practitioners of that specialty. Additionally, due professional care applies to the exercise or professional judgment in the conduct of work performed.
>
> Attention should be made to two important and distinctive points in these definitions. Due care are steps that are taken to show that appropriate individuals within an organization have taken responsibility for the activities that take place within the organization and have taken the necessary steps to help protect the organization, its resources and its mission.

The Due Care definition should include a footnote to ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an Information Security Management System.

F. Clarifying Figure 2-1

The term "automated records management" should be removed from text on the left hand side of the pyramid on p. 8 as the term does not appropriately captures the type of data that is pushed up from Tier 3. Can security facts truly be automated?

G. Section 3.1.2 Information System (Tier 3) Continuous Monitoring Strategy

The portion of Section 3.1.2 that states that "system owners are typically given some freedom in determining how to best customize tool use…." should be enhanced and clarified by including language explaining that tools are customized based on assessment results or other criteria.

As Section 3.4 of SP 800-53 notes, "[t]he continuous monitoring program includes an ongoing assessment of security control effectiveness to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment of operation. In particular, the organization revisits on a regular basis, the risk management activities described in the Risk Management Framework." Therefore, the requirement and guidance for customizing tools has been there, in some form, all along. One potential issue that should be considered is that an organization can be more focused on completing a paper-driven exercise of performing certification and accreditation than on continuous identification and control over risks to ensure that appropriate security controls are employed and functioning. While an organization may have certified and accredited all of its systems as required, none of the systems may actually be secure.

The SP 800-137 guidance document should encourage all agencies to reach government-wide agreements on identifying attack-based metrics by establishing a baseline of information security measures and controls that can then be continuously monitored through automated mechanisms. The section identified as the Information Systems level (Tier 3) on Page 18 scratches the surface on this topic but it fails to note the major differences between continuous control monitoring and continuous monitoring or inspection of business operations/processes. The generally accepted definition of continuous monitoring or continuous control monitoring as defined within this publication consists of activities focused on obtaining assurance that controls are operating the way they should. On the other hand, the continuous inspection or monitoring of business operations/processes is focused on testing processes for integrity after they have been processed.

Management uses technology to capture selected data and verify that the data is "correct." The intent is to detect errors, either to identify potential inconsistencies, or to identify the need for process improvements to prevent additional errors. Therefore, this distinction should be made in the document since there is a great deal of difference between tests that are intended to confirm controls are in place and tests that inspect data after the fact to ensure it is valid and correct. There is no such thing as continuous control monitoring/operations. The two should be clearly noted as follows:

1) Continuous control monitoring, otherwise known as continuous monitoring where all applicable controls are tested with respect to the FIPS199 categorization of the system/application in question; and

2) Continuous operations monitoring where the integrity of data and information are evaluated.

Both control monitoring and operations monitoring can relate to any type of control or organizational process, for the purpose of managing any form of risk. Continuous operation monitoring is a powerful detective control that should be considered in the design of internal controls, especially relative to data integrity. Whereas continuous control monitoring provides assurance that controls are in place to prevent or detect future business process or data errors. Realizing that it may not be feasible or cost-effective to monitor all of the security controls in an information system on a continuous basis, the information system owner/operator of each respective system/application should select an appropriate subset of those controls for periodic assessment.

H. Section 3.1.3 Define Sample Populations

The discussion should explain that Business Impact Analysis (BIA), discussed in Section 3.2 of NIST SP 800-34 Rev.1, will help in determining assets for sample population.

BIA is performed in an organization during the first stage of the business continuity management process. The goal of BIA is to identify relevant processes and to determine their criticality and subsequently potential impacts resulting from unavailability of such process from disruption of production or provision of services.

I. Vulnerability Information

In Footnote 35 on page 29, NIST should include, in addition to the NIST National Vulnerability Database, references to information concerning Common Vulnerabilities and Exposures, http://cve.mitre.org/cve/, and the Common Vulnerability Scoring System (CVSS), www.first.org/cvss.

J. Change Control Board

The document should include a statement explaining that proposed changes made to an organization's information systems potentially affecting continuous monitoring should be brought to a Change Control Board (CCB). A CCB should review and approve all changes needed for security purposes.

CCBs are an important practice for helping ensure management visibility and control of project requirements and scope changes. CCBs have the potential to reduce/prevent uncontrolled changes to the product and help ensure that the appropriate stakeholders have a say in project tradeoffs; therefore, it important to involve the right set of representatives to fully analyze the impact of requested changes.

Proposed changes presented to CCBs should be analyzed from the perspective of how scheduling, cost and other related features may be affected. The analysis function is one aspect to a CCB, another aspect would be the power to accept, modify or reject each proposed change. A discussion of CCBs within SP 800-137 should explain that all relevant team members need to be kept fully aware of each request status to prevent redundant requests and help ensure that CCB decisions are adhered to in a timely manner.

Moreover, the guidance document should explain that CCBs should have a formal process to facilitate change request and the performance of these changes. Possessing a written change control process ensures that the requests are handled efficiently, on schedule, include all necessary stakeholders and are decided on a reasoned basis. The change control document should outline the specific change request process, so team members are aware of what they need to do to submit the change request, and how to track the change request until its conclusion. The procedure should outline the necessary criteria for requesting the change as well as describe the flow process after the request has been submitted.

In addition, the term Change Control Board should be referenced in the Glossary in a manner similar to what follows:

> ***Recommended Definition of a Change Control Board***: Organization officials who meet to review all security change requests. Other CCB responsibilities include scheduling the change, communicating the change to all affected parties and coordinating user training. Membership should include senior officials representing each relevant organizational function.

K. Section 3.5 Analyze Data and Report Findings/OMB Memorandum M-10-15

A discussion should be added to section 3.5 which discusses the relevance of OMB Memorandum M-10-15, "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" to continuous monitoring. A footnote to the Memorandum should be included.[11] The guidance document should explain that the OMB directive requires that for "FY 2010, FISMA reporting for agencies through CyberScope, **due November 15, 2010**, will follow a three-tiered approach:

1. Data feeds directly from security management tools
2. Government-wide benchmarking on security posture
3. Agency-specific interviews" [Emphasis in original]

Of particular importance, SP 800-137 should explain that because of the requirement for data feeds directly from security management tools, OMB has instructed that "[a]gencies should not build separate systems for reporting. Any reporting should be a by-product of agencies' continuous monitoring programs and security management tools."

---

[11] Found at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

SP 800-137 should be updated as needed to incorporate new and/or revised OMB instructions to agencies relevant to continuous monitoring.

L. Appendix D.2 Technologies for Aggregation and Analysis

A new section should be to the Appendix D, D.2.x Future Implemented Controls. There should be three elements to this new sub-section as illustrated below.

Recommended Section D.2.x

Maintenance. It should be practical to establish hardware maintenance and configuration management standards for each platform. Platform sensors should be able to record maintenance actions and determine whether hardware maintenance and configuration are up-to-date. Discrepancies exceeding pre-defined limits are to be reported upon as a finding, as would maintenance events not corresponding to authorized actions.

Analysis of Audit Logs. The accepted best engineering practice for analyzing audit logs calls for logs to be examined on a regular and timely basis and for recorded events to be assigned a severity level. High-severity audit events should be reported to appropriate administrators immediately and identified as traceable action items, requiring analysis and closure within a specific, reasonable time period. It may be possible to automate the audit log analysis process, including the reporting, analysis, and resolution of high-severity audit events. Platform sensors could determine whether the logs are being examined regularly and whether high-severity audit events are being closed within the required periods. If the logs are not being appropriately examined, the sensors should report the non-action to one or more senior officials.

Identity and Access Management. There is little currently available in the way of automated continuous monitoring of identity and access management. These are potentially significant problem areas and research into them should be extensive and continuing, especially regarding ways of verifying their correctness and reducing their complexity. Future product offerings may include automated identification of erroneous access control assignments or of weak or compromised identity management, especially if standards for such things could be developed as Configuration Baselines. Such identity and access management features should be considered for implementation when feasible from a technical and budgetary standpoint.

V. Data Quality Act Compliance

As an official publication of a federal agency, the SP 800-137 document will be subject to the requirements of the Data Quality Act (DQA) and OMB and NIST implementing guidelines.[12] The document will also, if needed, be subject to the DQA's administrative correction procedures.

Two specific Data Quality issues to which we call NIST's attention:

1. Ensure compliance with the DQA's definition of utility. NIST's Guidelines define utility as referring "to the usefulness of the information to its intended users, including the public. In assessing the usefulness of information that the agency disseminates to the public, NIST considers the uses of the information not only from its own perspective but also from the perspective of the public."

   CRE has provided NIST with three possible enhanced definitions of continuous monitoring to help the agency achieve compliance with the utility requirement.

2. Statements indicating statutory compliance. In order for the document to be able to state or otherwise indicate that it is consistent with law, it will need to ensure compliance with FISMA's "equivalent levels of protection" flexibility requirement.

   CRE has provided NIST with the outlines a recommended "substantial equivalence" program to assist the agency in complying with FISMA requirements.

CRE recommends that NIST include a statement verifying that the document has successfully passed NIST's pre-dissemination review process. As NIST's DQA Guidelines explain, "[q]uality will be ensured and established at levels appropriate to the nature and timeliness of the information to be disseminated. Information quality is an integral part of the pre-dissemination review of information disseminated by NIST."

---

[12] OMB Guidelines found at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/reproducible2.pdf
NIST Guidelines found at http://www.nist.gov/director/quality_standards.cfm

VI. Summary of Key Recommendations

Prior to publication of Final Public Draft of SP 800-137, NIST should:

- Publish all comments received on the Initial Public Draft – these comments should be made public as soon as possible.
- Include a "substantial equivalence" provision that allows for alternative solutions using off-the-shelf security products to meet an organization's continuous monitoring needs.
- Begin development of a program to verify an organization's substantial equivalence security assurance for continuous monitoring.
- Enhance the definition of continuous monitoring to provide substantially greater specificity to:
  - Ensure that continuous monitoring solutions can detect patterns associated with insider threats as well as external threats and safeguard against both; and that
  - Continuous Monitoring means real time reporting with the ability to do *ad hoc* searching for forensic and monitoring purposes.
- Ensure the document complies with NIST Data Quality standards and include a statement attesting that it has successfully completed the agency's pre-dissemination review process.