

LA-UR-13-21921

Approved for public release; distribution is unlimited.

Title: Continuous Monitoring And Cyber Security For High Performance Computing

Author(s): Malin, Alex B.
Van Heule, Graham K.

Intended for: Workshop on Changing Landscapes in HPC Security (CLHS) 3013, 2013-06-17 (New York, New York, United States)

Issued: 2013-08-02 (Rev.1)



Disclaimer:

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the Los Alamos National Security, LLC for the National Nuclear Security Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Continuous Monitoring And Cyber Security For High Performance Computing

Alex Malin
Los Alamos National Laboratory
amalin@lanl.gov

Graham Van Heule
Los Alamos National Laboratory
grahamvh@lanl.gov

ABSTRACT

Continuous monitoring represents a potentially significant paradigm shift for cyber security as practiced throughout the US Federal Government. With continuous monitoring, rather than test a system once every three years during certification and accreditation, the security controls that are most vital and most volatile in a computer system are tested continuously to assure a high level of system security. A key goal is to provide near-real time security status-related information to organizational officials so they may take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information systems.

Continuous monitoring implementation has initially focused on desktop computer systems. Designing a solution to continuously monitor servers will be considerably more complex and challenging. The challenge will be even greater for computers used for scientific instrumentation and experimentation. This paper describes the challenges of adapting and applying the new cyber paradigm of continuous monitoring for supercomputing. It describes research at Los Alamos National Laboratory intended to develop an approach to continuous monitoring appropriate for supercomputers.

Categories and Subject Descriptors

D.4.6 [Security and Protection]: Verification

Keywords

Continuous monitoring, supercomputer, cyber security

1. INTRODUCTION

Continuous monitoring is a key component in the new US government cyber security governance model, the *risk management framework*. Rather than testing a system once every three years during certification and accreditation, a system is tested continuously and throughout the system lifecycle.

Copyright 2013 Association for Computing Machinery. ACM acknowledges that this contribution was authored or co-authored by an employee, contractor or affiliate of the U.S. Government. As such, the Government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for Government purposes only.

CLHS'13, June 18, 2013, New York, NY, USA.

Copyright © 2013 ACM 978-1-4503-1984-3/13/06...\$15.00.

According to NIST 800-37, Appendix G,[5] the objective for the continuous monitoring program is to determine if the set of deployed security controls continue to be effective over time. Continuous monitoring provides the authorization official information directly pertinent to the reauthorization decision, and provides near-real time security-status-to organization officials so they may take appropriate risk mitigation actions. Agencies have been directed by OMB to develop and implement continuous monitoring strategies for all information systems.[9] The Department of Homeland Security is coordinating mandated, automated FISMA reporting.

Given this new cyber governance model, what impacts may we anticipate for cyber security for supercomputers? This paper examines likely impacts, examining continuous monitoring from both compliance and technical cyber perspectives.

Though continuous monitoring is intended to replace compliance with risk-based cyber security,[3] there are significant challenges that have skeptics concerned that the US government may merely increase the compliance burden, adding new FISMA reporting requirements[4] without tangibly improving computer security. A key concern for supercomputing is that baseline requirements designed for desktop computers may become requirements for supercomputers that would be inappropriate and ineffective. For example, it seems likely that anti-virus tools will be a required component of the cyber health report scorecard for desktop computer systems. Supercomputing centers may feel pressure to deploy host-based vulnerability scanners, antivirus, and other COTS tools as continuous monitoring becomes mandatory.

2. EARLY IMPLEMENTATION

A consortium from government, industry, and academia is working out technical details and standards for implementing continuous monitoring. The idea is to collect inventory, configuration, and vulnerability data, for example, about a host, determine if a host meets compliance requirements (USGCB,[8] FISMA, etc.) and produce reports used by managers responsible for cyber risk throughout the US government. Summary reports are sent from sites to central database systems at each agency, then reported by agencies to OMB.

The national effort has focused initially on monitoring desktop computers. NIST-approved configuration baselines have been approved for Windows desktop and RedHat Enterprise Linux (RHEL) desktop machines. To date there are

no US Government Configuration Baseline (USGCB) standards for Unix servers. There is sufficient challenge and complexity to designing and deploying a system of continuous monitoring for desktop computers; one could reasonably conclude that it may likely be several years before standards are established for servers.

3. HPC CONTINUOUS MONITORING

The complexity and challenge of continuously monitoring high performance computing (HPC) with COTS tools is illustrated by the example of the Tripod Operating System Software (TOSS),[1] a customized RedHat Linux (RHEL) operating system with a modified kernel that is optimized with an HPC application environment. TOSS is deployed on many commodity-based clusters at Los Alamos National Laboratory (LANL), Lawrence Livermore National Laboratory, and Sandia National Laboratories. Once USGCB standards are approved by NIST for Linux servers, and once vendors have developed COTS tools for standard RHEL servers, these COTS tools would likely need extensive adaptations and modifications to report valid security scores for HPC systems. It is uncertain whether COTS tools and Cyber-Scope,[6] the DHS central reporting infrastructure, will be configurable to the degree needed to report an accurate and valid status on the security of HPC systems. It should be noted that NIST-approved configuration baselines and associated COTS tools may never be developed for some specialized, vendor supported and experimental HPC systems and infrastructure components operated at US government national laboratories.

Considering these challenges, the path of least resistance would perhaps be to take a passive approach, wait while USGCB standards evolve and see how the COTS market develops. Implementation of continuous monitoring is still relatively new and has not been fully funded. Supercomputing sites could perhaps seek exemptions to government requirements for continuous monitoring while standards and markets evolve.

This paper proposes that US government organizations with HPC assets take a more proactive stance. It may be well worth the effort to work at the bleeding edge of continuous monitoring for its potential to tangibly improve HPC technical security and streamline HPC compliance. There is risk that a desktop-focused solution may set new requirements for HPC that would be ineffective and costly. While the national focus is on monitoring desktop systems, HPC sites have an opportunity to influence national decision-makers to account for differences between desktop computing and servers, and between COTS computing and HPC and other iterations of scientific computing systems.

3.1 Technical Objectives

This section explores the technical and functional objectives for continuous monitoring and how these may be applicable to HPC. The primary resource used here is a draft document describing technical requirements for continuous monitoring, published by the Department of Homeland Security (DHS).[2] This document is marked *pre-decisional working draft for discussion only*. The document has no formal title or publication date.

The tentative nature of these qualifiers is both revealing and relevant to our analysis of the applicability of technical objectives for continuous monitoring to HPC. The objectives

for continuous monitoring are beginning to be clear though these are still in a formative state. Its implementation is just beginning to evolve.

The DHS working draft covers four technical areas, hardware inventory, software inventory, configuration management, and vulnerability management. The inventory areas seem to have less relevance to HPC security. Configuration and vulnerability management seem to have more relevance.

3.1.1 Hardware Inventory

According to the DHS working draft, “The objective of the hardware inventory management function is to discover and remove unauthorized or unmanaged hardware on a network. Since unauthorized hardware is unmanaged, it is likely vulnerable and will be exploited as a pivot to other assets if not removed or managed.”

Supercomputers and the file systems and network infrastructure that support HPC are quite expensive, compared with a single desktop computer, mobile computing device, or server. Extensive organizational resources are brought to bear when new HPC equipment is purchased, integrated, and supported in production. The likelihood is quite low that a new supercomputer would be deployed without being authorized or managed. This applies to the high performance switch fabric, and file systems that support HPC.

We assert that the hardware deployed by HPC organizations is all *managed*. The likelihood of deploying an unmanaged server in an HPC environment seems very low.

3.1.2 Software Inventory

According to DHS working draft, “The objective of the software inventory management function is to discover and remove unauthorized or unmanaged software configuration items in IT assets on a network. Because unauthorized software is unmanaged, it is probably vulnerable to being exploited as a pivot to other IT assets if not removed or managed. In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings; malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate itself throughout the enterprise.”

The DHS working draft asserts that unmanaged software, like unmanaged hardware, is more likely to be poorly managed and therefore vulnerable to exploitation. This seems plausible for desktop and mobile computing. As we demonstrated in the hardware inventory discussion above, HPC is managed environment, rendering these considerations less applicable.

The DHS working draft also asserts that a complete and accurate software inventory supports an effective configuration management and vulnerability management program. This aspect of software inventory for continuous monitoring seems to have greater potential relevance for supercomputing. One needs to have a handle on the software environment to configure software securely, to keep cognizant of software vulnerabilities and to remediate vulnerabilities in a timely manner. Configuration management and vulnerability management are covered in sections 3.1.3 and 3.1.4 below.

3.1.3 Configuration Management

According to DHS working draft, “The objective of the

configuration management function is to reduce misconfiguration of IT assets, including misconfigurations of hardware devices (to include physical, virtual and operating system) and software. Over 80 percent of known vulnerabilities are attributed to misconfiguration and missing patches. Cyber adversaries often use automated computer attack programs to search for and exploit IT assets with misconfigurations, especially for assets supporting federal agencies, and then pivot to attack other assets.”

Of the four technical areas in the DHS working draft, configuration management perhaps has the most relevance for HPC continuous monitoring. Misconfigurations (or the absence of robust configuration management) can create exploitable weaknesses in HPC environments. Best practices in configuration management, including automated tools like cfengine or puppet, and mature change management processes, can prevent exploits from executing, can minimize the spread of an attack, and can be leveraged to detect attacks in progress.

Early tests at LANL to deploy continuous monitoring for HPC have focused primarily in the area of configuration management. These tests and related analysis will be described in sections 4 and 5 below.

3.1.4 Vulnerability Management

According to DHS working draft, “The objective of the vulnerability management function is to discover and support remediation of vulnerabilities in IT assets on a network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified and removed or remediated quickly from operational systems so that they can no longer be exploited. (An information security vulnerability is a deficiency in software that can be directly used by a hacker to gain access to a system or network.)”

Effective vulnerability discovery and remediation tools and processes can tangibly strengthen HPC security. As continuous monitoring COTS tools mature, these tools could be valuable for HPC.

3.1.5 Anti-virus

It is perhaps surprising that anti-virus was omitted from the DHS working draft. Anti-virus is often included as a core area for continuous monitoring.[10] We may assume that anti-virus software will likely be required to continuously monitor desktop computers, that dashboards will report whether anti-virus tools are present and whether definitions are up-to-date. It is not unusual for policy makers and oversight officials to promote a one size fits all security model, which assumes that security controls that protect desktop systems should also be deployed on servers and on HPC systems. We assert that anti-virus products have little relevance for the security of Unix servers, yet they are required in some environments for compliance purposes.

One of the best arguments for HPC to actively engage in developing an approach to continuous monitoring that is relevant and meaningful to HPC is to prevent the proliferation of anti-virus-like tools on HPC systems. Articulating and communicating the distinctions between HPC and desktop computing to policymakers and oversight officials could prove highly beneficial; however, it may not be good enough to simply say what will not work for HPC. A key premise

of this paper is that an HPC strategy for continuous monitoring should focus on monitoring mechanisms that make a tangible difference to HPC security.

4. PROOF OF CONCEPT

LANL HPC began developing new continuous monitoring capabilities in 2011. This section describes these initial experiments. However, we prefer not to discuss the LANL HPC cyber security posture in an open publication. Therefore, this paper will describe continuous monitoring hypothetically.

Continuous monitoring potentially will shift time and money away from compliance and toward expenditures and effort that tangibly strengthen system security. While there may be legitimate skepticism whether the US government can wean itself from the compliance mindset, the LANL initial foray into continuous monitoring was designed to tangibly improve cyber security. Two questions guided the LANL selection of security mechanisms for continuous monitoring: 1) What security mechanisms tangibly strengthen HPC security, and 2) Which of these mechanisms can most readily be automated to monitor continuously.

The examples that follow fall into the area of configuration management, described in 3.1.3 above. Of the four technical areas in the DHS working draft, configuration management perhaps has the highest potential for strengthening HPC cyber security. Continuous monitoring focused in the area of configuration management ensures that configuration settings pertinent to security are properly set, and prevents misconfigurations that may negatively impact system security. The monitoring of these security-related controls has both preventative and detective potential benefits.

A. Host-based firewalls are a basic and important preventative control. A malicious actor may attempt to change the firewall configuration, or may stop the firewall service. A hypothetical continuous monitoring tool runs tests to verify that a host-based firewall is running. It compares stored and running configurations to ensure the correct configuration is in place. And it tests that the firewall in fact blocks traffic that it should be blocking.

B. Many HPC sites deploy automated configuration management tools such as cfengine or puppet to ensure that a system boots and runs with a baseline configuration, and to restore the configuration if it changes improperly. A hypothetical continuous monitoring tool adds a preventative check to ensure that HPC configuration management tools run at the correct time interval, and adds a detective capability by monitoring logs to identify when unauthorized changes are made on the system.

C. A malicious actor may attempt to open an unauthorized service on a system to maintain a persistent presence or to exfiltrate information. A hypothetical continuous monitoring tool monitors the services running on the system and compares these with a baseline. Unauthorized changes are reported.

D. HPC systems run a variety tools designed to detect malicious activity. A malicious actor may attempt to disable security tools to avoid detection. A hypothetical continuous monitoring tool checks that intrusion detection and malicious code detection tools are operating correctly and reports when they do not.

5. HPC TOOLS RESEARCH

As described in section 3.1 (above), DHS has initially focused on four areas to implement OMB-required continuous monitoring: hardware asset management, software asset management, configuration management, and vulnerability management.

This paper has advocated for an approach to continuous monitoring that sets priorities, monitoring things that tangibly improve HPC cyber security. We next examine tools and approaches for their potential applicability for HPC continuous monitoring. We also identify areas for potential collaboration and research.

5.1 Hardware Inventory Tools

In section 3.1.1, we asserted that the hardware deployed by HPC organizations is all *managed*. If this analysis is correct, hardware inventories have less relevance to the security of HPC systems. Never the less, hardware inventories are typically required for cyber compliance. Organizations that support HPC currently address this requirement in some form or another. For compliance only, it may well be in the interests of HPC to automate the collection and reporting of hardware inventory, for continuous monitoring, provided that this may be done relatively cheaply and easily. Alternatively, some HPC organizations may choose to pursue an exception to the requirement to monitor hardware continuously.

To address continuous monitoring requirements, we anticipate that government organizations will likely roll out in-house developed or off-the-shelf tools to collect and report hardware inventory. The data would be used in-house to support risk mitigation efforts. A subset of data would be shipped to agencies and DHS using CyberScope.

Installing hardware inventory agent software in the supercomputing environment may not be relevant or appropriate. The simplest and cheapest approach for HPC may be to work with host organizations to ensure that site-wide tools provide an API that would allow HPC to send hardware inventory information to a central database. Defining what constitutes a hardware asset for HPC is a crucial decision, when we consider that hardware parts are replaced frequently in HPC systems. HPC does not want a dashboard to go red whenever technicians swap out a motherboard or replace a compute node.

It seems unlikely that it would be worth the expenditure of time or effort for HPC sites to purchase or build in-house tools specific to the needs of HPC for continuously monitoring hardware inventory. It may be worthwhile for HPC sites to collaborate in defining the hardware inventory in a common manner. From a FISMA perspective, it perhaps makes most sense to list a supercomputer as a single hardware asset.

5.2 Software Inventory Tools

Similar to the hardware inventory, section 3.1.2 above asserted that in HPC environments, software is *managed*; the concern that unmanaged software may lead to software flaws seems irrelevant for HPC. Never the less, there are areas associated with software inventory that may have relevance for HPC security. There is potential value in knowing what software is deployed to configure this software securely, and to keep cognizant of software vulnerabilities to remediate vulnerabilities in a timely manner.

A discussion on tools and techniques to continuously monitor the management of configurations and vulnerabilities will follow in sections 5.3 and 5.4. For HPC systems, we assert that software inventory agent software should be tightly integrated with configuration and vulnerability management to be relevant. A software reporting tool that is independent and merely reports software changes may have less value in the HPC context. An HPC software inventory capability should be able to distinguish between software installed in user space and software installed in the system area. Users of HPC systems install and run software at their discretion. A red dashboard any time a user installs software would be counter productive. On the other hand, a software monitoring tool may be useful if it establishes a baseline for software running as root, and keeps cognizant of changes to this baseline and installation of new software added to the system area.

5.3 Configuration Management Tools

This paper has advocated an approach to HPC continuous monitoring that emphasizes configuration management. Misconfigurations (or the absence of robust configuration management) can create exploitable weaknesses in HPC environments. Best practices in configuration management, including automated tools like cfengine or puppet, and mature change management processes, can prevent exploits from executing, can minimize the spread of an attack, and can be leveraged to detect attacks in progress.

Once USGCB standards are approved by NIST for Linux servers, and once vendors have developed COTS tools for standard RHEL servers, these COTS tools would likely need extensive adaptations and modifications to report valid security scores for HPC systems. This points to potential value for research and collaboration among HPC sites in the area of continuous monitoring of system configuration. HPC experts would be best qualified to USGCB standard for Linux servers to be relevant for HPC.

Considering the diversity of HPC systems, is there potential for a USGCB standard that could capture a baseline security configuration of Linux supercomputers? If this can be developed, what is the potential for a COTS tool to implement this in a continuous monitoring framework? Or should HPC sites collaborate to develop custom continuous monitoring tools that are sufficiently flexible to be used at diverse HPC sites? Whether COTS or in-house, these tools would need to endeavor to accurately reflect the security of HPC systems.

For its initial experiments, LANL HPC deployed an in-house developed tool for continuous monitoring of configurations. The tool has been a success thus far in that it integrates into the LANL HPC environment and meets performance metrics. However, an in-house developed tool has potential pitfalls. There is the question of sustainability. Would the homegrown tool survive a change in personnel? Is it documented well enough? Would a more standards-based, COTS tool provide greater capability out of the box. We are not aware of any COTS tool that could be integrated into the LANL HPC environment and that has the capabilities and flexibility required. However, we expect the market to mature and are interested to see which vendors commit to address Linux server security.

5.4 Vulnerability Management Tools

There may well be COTS tools currently on the market that would provide on-host vulnerability testing of Linux servers that have capability to report in standards-based language to the DHS CyberScope.

There are several important caveats to keep in mind as continuous monitoring requirements and tools are deployed. System stability is paramount in HPC environments. Routine operating system and software updates require extensive testing before they can be applied to HPC systems, and cannot be applied as quickly as desktop systems. Vulnerability remediation is typically handled faster for desktop systems than for servers and HPC systems.

There are key differences in the threat environment on HPC systems as compared to desktop systems. The principal threats to desktop and mobile computers, related to browsing the web and client-based email, are not typically relevant to HPC. Privilege escalation attacks are a much greater concern on multi-user HPC systems. To have relevance for HPC, the COTS tools that provide notification of software vulnerabilities would need to reflect the proper severity weighting of these vulnerabilities. The COTS tools selected for the broader enterprise may be able to provide valid vulnerability information for HPC, if the severity ratings may be flexibly configured. If the enterprise selects a continuous monitoring tool primarily for its relevance to Windows desktop computing, or if staff lack the training and knowledge to tune these COTS systems for various environments in the enterprise, HPC organizations may need to select a different set of vulnerability assessment tools for these tools to be useful. This may be cost prohibitive for some organizations.

HPC sites may benefit from research and collaboration in the area of on-host vulnerability monitoring. As organizations test vendor products for suitability for HPC, sites could benefit by collaboration and information sharing.

Continuous monitoring provides near-real time security status-related information to organization officials so they may take appropriate risk mitigation actions. As COTS tools mature, they will likely feed dashboards that report this status, perhaps expressed visually as green, yellow and red alarms. If the COTS tools are not configured to accurately reflect the relevance of software vulnerabilities for HPC, organization officials may see alarms for HPC systems that should not or cannot be remediated in a timely manner. If red alarms are reported to agencies and to OMB, these red alarms may not accurately reflect the security state or the business requirements of HPC systems.

6. REPORTING RESULTS

At some point, HPC organizations will need to find some means to report continuous monitoring results in a manner that is compatible with SCAP[11] and XCCDF[7] standards used to report to the DHS tool, CyberScope. This is where the rubber really meets the road, so to speak, and the challenges are substantial. Will there be some way to both test security controls that are relevant and meaningful to HPC security, and report this to a dashboard tool that shows green, yellow and red accurately and appropriately? Or will HPC organizations bite the bullet once again and deploy agents and tools that do not help security but buy a measure of compliance?

7. COMPLIANCE

This paper has focused primarily on technical security. Continuous monitoring has the potential to change the compliance landscape. This will likely have implications in supercomputing.

7.1 Streamlining Cyber Compliance

According to NIST 800-37, Appendix G,[5] the objective for the continuous monitoring program is to determine if the set of deployed security controls continue to be effective over time. Continuous monitoring provides authorization officials information directly pertinent to the reauthorization decision, and provides near-real time security status-related information to organization officials so they may take appropriate risk mitigation actions. Continuous monitoring represents a new compliance paradigm, where the three-year certification and authorization cycle is replaced by continuous monitoring.

“The ultimate objective is to achieve a state of ongoing authorization where the authorizing official maintains sufficient knowledge of the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system) to determine whether continued operation is acceptable based on ongoing risk determinations, and if not, which step or steps in the Risk Management Framework needs to be re-executed in order to adequately mitigate the additional risk.”[5]

Continuous monitoring has the potential to reduce compliance costs by eliminating the requirement to write, review and approve a new security plan every three years. So long as a system meets criteria to maintain approval status, authorization will be continuous. Continuous monitoring also has the potential to reduce costs associated with testing systems for certification and accreditation by automating tests that currently involve manual tests and documentation.

The Office of the CIO at Los Alamos estimates that the average cost for system certification and accreditation is 300,000 US dollars. Complex systems can cost 500,000 US dollars or more. Eliminating the requirement for new security plans could lead to considerable cost savings for HPC. On the other hand, depending on its implementation, the new *risk management framework* and continuous monitoring could add additional compliance requirements, without substantially reducing current compliance requirements. There would continue to be costs to keep a security plan up to date over an extended period of time. We also anticipate costs associated with new documentation and new tools that support continuous monitoring.

Automation of testing NIST 800-53 controls can replace manual testing, during the initial certification and accreditation, and as new supercomputers are rolled out. System testing for certification and accreditation is currently a manual process at LANL, where HPC re-tests all system components every three years. In 2011, local cyber oversight required testing of more than 400 NIST 800-53 controls. LANL also manually tests a set of NIST 800-53 controls each time LANL brings up a new supercomputer.

NIST 800-37 does not require require continuous monitoring of every NIST 800-53 control. Authorizing officials may approve a limited set of controls for continuous monitoring, allowing organizations to focus resources where they are most effective. The volatility of cyber security controls may be evaluated to establish an appropriate frequency for

monitoring. Controls that are more likely to change would be tested more often. Controls that are static would be tested less often. The value of a control to making the authorization decision could also be considered. Lower priority controls could be tested once, during initial certification and accreditation. Higher priority controls could be monitored continuously, at a frequency based on their volatility and value.

Continuous monitoring is designed to be flexible. However, we may find that site cyber security officials, oversight officials and auditors may not easily shake the compliance mindset.

7.2 Compliance Costs

While continuous monitoring has the potential to reduce costs for compliance, it will create new requirements, which in some agencies and organizations, could increase rather than reduce costs.

To implement continuous monitoring, organizations will develop new processes to provide authorization officials status updates on control effectiveness and other information pertinent to the reauthorization decision. It seems likely that new documentation will be required to supplement the security plan and keep authorization officials well informed. This could include a synopsis on recent audit assessments and findings, status on security controls identified as weak in previous assessments, and changes in system risk profile. Control automation and dashboards will likely be phased in over time to replace manual testing and some of this documentation. Some controls do not lend themselves well to automation and may remain manual indefinitely. Decisions made at the agency and site levels will impact the costs associated with new documentation for continuous monitoring, and documentation costs are reduced or increased.

Automation itself carries a cost. Most costs associated with continuous monitoring compliance will likely be associated with building, buying, integrating and maintaining automated tools for monitoring and reporting. To the degree that HPC organizations can leverage tools deployed at their respective institutions and by agencies themselves, these costs will not be borne directly by HPC. As we discussed in Section 5 (above), HPC may need to develop and maintain in-house solutions for automated continuous monitoring, where COTS tools may not work, or may impede with operations of supercomputers. To the degree that continuous monitoring tangibly improves security, these costs will be easier to swallow. If continuous monitoring becomes just compliance, the costs for compliance will likely continue to rise.

7.3 National Trends in Compliance

While agencies are being directed to risk-based policies and controls, it remains to be seen whether the perspectives of decision-makers will change. Will the *Risk Management Framework* and *Continuous Monitoring* improve the security of federal systems, or merely change compliance and reporting requirements? Will costs shift away from compliance and toward security that adds tangible value? Will costs for compliance increase or decrease? Will success be measured by compliance with reporting requirements, or with how well sites use monitoring information to improve system security? OMB is requiring agencies to report on security metrics to comply with FISMA; it is unclear whether OMB has the

leverage to ensure that agencies are using these metrics to reduce risk to computer systems.

8. CONCLUSIONS

This paper has described the challenges of adapting and applying the new cyber paradigm of continuous monitoring for HPC, and has described research at Los Alamos National Laboratory intended to develop an approach to continuous monitoring appropriate for supercomputers. We explored how compliance may change, and described the technical objectives for continuous monitoring. While continuous monitoring in the areas of configuration management and vulnerability management has potential to improve HPC security, the COTS tools and NIST-approved benchmarks are currently designed for desktop computer security environments. This paper has advocated for a proactive rather than a reactive approach for US government organizations that manage HPC systems. We believe there is significant potential for HPC sites to collaborate on approaches, tools and techniques to meet compliance requirements and strengthen cyber security in ways suitable for HPC systems.

9. REFERENCES

- [1] CHAOS. Linux distribution for high performance computing. http://code.google.com/p/chaos-release/wiki/CHAOS_Description/.
- [2] DHS. Draft technical requirements. <https://www.fbo.gov/utills/view?id=ae650dd0661deab13c6805f94a542a>
- [3] NIST. Frequently asked questions continuous monitoring. <http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf>.
- [4] NIST. Fy 2012 reporting instructions for the federal information security management act and agency privacy management. <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012-20.pdf>.
- [5] NIST. Guide for applying the risk management framework to federal information systems. <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>.
- [6] NIST. Security content automation protocol. scap.nist.gov/use-case/cyberscope/.
- [7] NIST. Specification for the extensible configuration checklist description format (xccdf) version 1.2. <http://csrc.nist.gov/publications/nistir/ir7275-rev4/NISTIR-7275r4.pdf>.
- [8] NIST. The united states government configuration baseline (usgcb). <http://usgcb.nist.gov/>.
- [9] O. of Management and Budget. Fy 2011 reporting instructions for the federal information security management act and agency privacy management. <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013-33.pdf>.
- [10] F. N. Radio. Dhs hones dynamic approach to securing agency computer networks. <http://www.federalnewsradio.com/473/2922072/DHS-hones-dynamic-approach-to-securing-agency-computer-networks>.
- [11] scap.org. Open scap. <http://open-scap.org/page/MainPage>.