Revision History

Revision Description	Author/Modifier	Version	Date
	Russ Hammond	1.0	
Section I.1 – added logging Section V – revised requirements	Russ Hammond	1.1	Nov 18, 2012
Revised to incorporate new information about M&A tool capabilities, new approach to M&A Section I: 1. Removed the pub/sub language 2. Replaced reference to reports with more generic language Section II: 1. Modified definition of an alert to differentiate from user notification 2. Added definition of a Notification Section III: 1. Added comment to #3 2. Revised #4 Section V: 1. Removed reqts RFP.88.1.2, RFP.88.1.3 – per conversation with David 2. Replaced RFP.88.1.5 with RFP.88.1.6 3. Removed RADMA.1.4, configurable retention for alerts, metrics, errors, logs 4. Removed RADMA.1.5 – Student and Proctor workstations will not use M&A 5. Added RADMA.1.6, RADMA.1.6.1 – deletion of messages through a UI 6. RADMA.7.1 – changed from pub/sub channel to notifying a group		1.2	March 8, 2013
Section V:	Russ Hammond	1.3	• March 20,

• Reqt RFP.88.1.6 – removed reference to users entering an email address – just require that notification be sent to an email address. Method of entering addresses is not yet determined. • Added reqts RFP.118, RFP.118.1, RFP.120, RFP.120.1, RFP.121, RFP.122 • RADMA.1.3 – modified to say that M&A persists messages, added comment • RADMA.1.6 – changed delete function reqt from “user” to “system administrator” • PRMA.2.2 – added “log messages” to reqt • PRMA.2.4 – added reqt to export search results to .CSV Section VI: • Removed Errors category from the Data Transfer listing.			2013
Section II: • Added defns for node, server, and source Section IV: • Added issue about what to do with MnA messages that have no source info Section V: • Added reqts RFP.121.1, RFP.121.2: require source info for an MnA message • PRMA.1.1 – reqt is met by Hyperic, no custom UI needed	Russ Hammond	1.4	March 28, 2013
Requirement changes after discussion in AIR/DRC tech meeting Section V. • Removed reqt RADMA.1.6, RADMA.1.6.1, PRMA.2.4	Russ Hammond	1.5	April 8, 2013
Section V: • Added RADMA.9 for browsers to be supported by UI	Russ Hammond	1.6	April 10, 2013
Section V:	Russ Hammond	1.7	April 16, 2013

• Removed reqts RFP.121.1, RFP.121.2. M&A Notification Rules can be created if desired by the user			

I. Introduction

1. The overall responsibilities of this component are:
    a. Allow any component to submit metrics
    b. Allow any component to submit error events
    c. Allow any component to submit alerts
    d. Allow any component to submit log messages
    e. Generate alerts based on logs, errors, metrics and alerts for reporting and the routing of notifications to users in a configurable manner
    f. Allow any component to store system logging in a centralized location for reporting and problem investigation.
    g. Allow users to access monitoring, alerting and logging information
    h. Distribute alerts to users and user interfaces
    i. Monitor the health of servers

The audience for Monitoring and Alerting is:

1) System Administrators – technical personnel responsible for keeping the system operating and available
2) Business users – those who need to be notified of the status, success or failure of an action they have taken to accomplish a business need (e.g. importing items to the Test Item Bank).

II. Terms and Definitions

Term	Definition
Alert	A warning message regarding the operation of the system that requires the attention of an administrator. Alerts can be created directly by components, or by the Monitoring and Alerting component itself by applying configurable rules to Metrics, Errors and Alerts.
Alert Rule	Alert generation can be rule based on such criteria as the count of an event in a time period, severity of event, or passing a threshold. Each component has been categorized as a High or Medium availability component, and there will be differing alerting needs for each category of component.
Error	Predetermined conditions under which the system cannot continue normal processing.
Log Configuration	Used by the centralized log configuration tool to specify logging level
Log Entry	An individual entry set to the Monitoring and Alerting component to be persisted for reporting and telemetry. Log entries are for information or debugging and do

	not include Metrics, Errors and Alerts.
Metric	A measure of system functioning, such as available memory, CPU utilization, query performance or component activity levels
Node	The instance of the operating system from which a message is sent to Monitoring and Alerting
Notification	A message to inform a user of the status of an action they have taken.
Runtime Exception	An unexpected condition that occurs during system operation for which no predetermined error exists
Server	The application which accepts requests, and runs on a node. For example, multiple instances of Tomcat running on one node represent different servers.
Source (of a Monitoring and Alerting Message)	The component which sent the message to Monitoring and Alerting
View	An entity that allows the display of Monitoring and Alerting information

III. Assumptions

	Assumption	Comments
1.	Runtime exceptions for all components will be written to Monitoring and Alerting.	
2.	Access to system logs and alerts will be controlled by user roles in the Permissions shared component.	
3.	The Monitoring and Alerting component can be implemented using an existing off-the-shelf package if the off-the-shelf product meets the requirements for Monitoring and Alerting.	Monitoring and Alerting will use off-the-shelf functionality to provide server health information, and custom code to provide notifications to business users.
4.	~~Front end components will send logging, metrics, errors and alerts to the back end component which will direct them to Monitoring and Alerting.~~ ~~Test Delivery, and the Student and Proctor Workstations will not use Monitoring and Alerting for reporting metrics, errors, alerts and logs.~~ Test Delivery will send alerts to the Proctor and Student workstations without using Monitoring and Alerting. Monitoring and Alerting will still be sent metrics and logging information from Test Delivery.	~~Per 2/7 tech meeting with AIR, comments by David~~ Per 3/6/13 conversation with David
5.	The component will be open-sourced when	DRC will deliver code to AIR, who will open

	completed	source the system

IV. Issues

	Issue	Status	
1.	What does an environment look like for Monitoring and Alerting? Will there be one Monitoring and Alerting at the Consortium level, or a Monitoring and Alerting at multiple levels. How will the different levels interact?	Open	11/11/2012 – Russ
2.	What is the identity of a metric/error/alert? How do we track these state/district/school, etc.	Open	11/12/2012 – Russ 03/28/2013 – Russ – every message sent to Monitoring and Alerting will have the name of the component, the server and the node as input parameters.
3.	How are components “registered” and identified within a deployment?	Open	11/14/2012 – Russ
4.	If Monitoring and Alerting receives a message without information to identify the source, what should it do with the message? What information can be stored, and to whom should the alert be sent?	Open	~~3/28/2013 – Russ – Message will be persisted as an alert, questions as to what we can store and whom should be notified~~. 4/16/2013 – Russ – Messages without origin information will be stored in logging. A notification rule can be written to create notifications from messages lacking origin information.

V. Requirements

Requirements are numbered according to the following convention:

3) RFP.## - a requirement from the RFP
4) RADMA.## - a requirement from the detailed requirements from RFP-11 or the Architecture document
5) PRMA.## - a requirement from the Proposal
6) NFRMA.## - a nonfunctional requirement

Source.ID	Requirement	Category	Priority	Comments
RFP.88	System includes a suite of alerts to the test administrator and Consortium delegates if there appears to be a testing irregularity.	Dashboard	High	Monitoring and Alerting will not be responsible for defining and identifying "testing irregularities". Monitoring and Alerting will be responsible for publishing an alert to the appropriate topic.
RFP.88.1	The System will support multiple administrative roles which will have access to different types and levels of monitoring and alerting information.	Dashboard	High	See the table in Section I for the defined roles.
RFP.88.1.1	The system will provide alerts needed for real-time preventive monitoring to system support personnel.	Dashboard	High	Events such as resource shortages, server health
~~RFP.88.1.2~~	~~The system will provide events needed for monitoring a component to a Component Administrator.~~	~~Dashboard~~	~~High~~	~~Someone in charge of test delivery or test authoring, etc.~~ 3/8/2013 – Will not have Component Administrator role.
~~RFP.88.1.3~~	~~The system will provide access logs and alerts to Security Auditors.~~	~~Dashboard~~	~~High~~	~~Login failures, password resets, etc.~~
RFP.88.1.4	The system will provide System Administrators with a listing of the components registered with Monitoring and Alerting and the component's health status.	Dashboard	High	See Reqt. RADMA.1.2. The user interface could be a simple grid of components and statuses represented as Green, Yellow, or

				Red.
RFP.88.1.5	~~The system will allow recipients of alerts to be configured with options for different methods of alert delivery.~~	Configuration	Medium	~~For example, email or text message~~.
RFP.88.1.6	The system will allow notifications to be sent to an email address.	Configuration	Medium	3/8/2013 –Will only require email notification since an email can be sent to a phone number as well
RFP.118	Sufficient audits must be available to identify the source and time of data changes related to system components. (3/20/13)	Monitoring	High	Individual components must log the data changes.
RFP.118.1	The system must allow components to record the source and time of data changes.	Monitoring	High	Components are responsible for issuing messages about data changes. Monitoring and Alerting must accept the messages.
RFP.119	System must ensure that it logs system activity necessary to monitor and debug the system in a timely and accurate manner.	Monitoring	High	Each component will be responsible for performing its own logging. Monitoring and Alerting will capture the information sent by components.
RFP.119.1	Logging information will be stored locally on any server hosting a component. The local logging file would not be accessible through the component; an administrator would log on to the server to view the file. The logging information will also be stored centrally to allow for convenient access.	Framework	High	The local repository will be needed in cases in which communication with the centralized store is severed.
RFP.119.2	The centralized logging data will be updated real-time.	Framework	High	
RFP.119.3	System will allow severity level of logging data collected to be changed while the system is operating without interrupting service to the business user.	Framework	High	Ex: Can change from WARN down to DEBUG back to WARN w/o stopping. Existing logs remain unchanged – the level of messages collected is changed, rather than filtering the view of the collected log messages
RFP.119.4	The system will support at least 4 severity levels of	Framework	Medium	

	log messages.			
RFP.119.5	The system will provide a user interface which allows authorized users to search alerts, metrics, logs, and errors.			3/8/13 – added
RFP.120	System must ensure that all errors are written to an error log. (3/20/13)	Monitoring	High	3/20/13 – added to Level II document
RFP.120.1	The system must provide the ability to persist error messages	Framework	High	3/20/13 – each component will need to log its errors. Monitoring and alerting will provide the means of persisting the error information.
RFP.121	Errors to the end user must be communicated in plain language with an explanation of required action. (3/20/13)	Monitoring	High	This is requirement must be met by clients of Monitoring and Alerting. Monitoring and Alerting will not alter messages received from other sources.
~~RFP.121.1~~	~~All messages sent to Monitoring and Alerting must contain the source component, server, and node.~~	~~Monitoring~~	~~High~~	~~3/28/13 – Need the appropriate information to trace a message to its source~~
~~RFP.121.2~~	~~If Monitoring and Alerting receives a message which is missing source, server, or node information, the message will be persisted as an alert~~	~~Monitoring~~	~~High~~	~~3/28/13 – open issue about how to handle the alert~~ 4/16/2013 – users can create a notification rule to find messages where no component, server or node is included.
RFP.122	System must allow for a system administrator to view, filter, sort, and search the error log. (3/20/13)	Monitoring	High	Included in RFP.119.5
RADMA.1	Provide a framework for other components' log information	Framework	High	See Reqts. RFP.119.1-4.
RADMA.1.1	Every server hosting a component will be monitored for performance statistics and exceptional conditions.	Framework	High	The Monitoring and Alerting component will aggregate information sent from servers.
RADMA.1.2	Monitoring and Alerting must record the status of all deployed components at a set time interval.	Monitoring	Medium	Time interval is TBD. 3/8/2013 - Components are available or not available. The time interval for checking status is

				dependent on the capabilities of the Hyperic tool.
RADMA.1.3	Each component must write any collected metrics, errors, and alerts to the Monitoring and Alerting component. Each component will have unique metrics, errors and alerts which depend on the purpose of the component. The alerts, errors and metrics will be defined in the component's requirements. Monitoring and Alerting must provide the ability to persist the messages sent by the components.	Monitoring	High	Components are responsible for sending messages to Monitoring and Alerting.
~~RADMA.1.4~~	~~The retention of log, metric, error and alert types can be specified independently of one another. The retention period selected for a type will apply to all messages of that type.~~	~~Configuration~~	~~Medium~~	~~Ex: Save Logs 7 days and Alerts for 3 months. All alerts will be saved for 3 months.~~ 3/8/2013 – Based on discussion with David, removed this requirement, added RADMA.1.6.
~~RADMA.1.5~~	~~System components not running on a server (such as the Student Workstation) must report logging, metrics, errors and alerts through the primary server components with which they communicate.~~	~~Framework~~	~~High~~	~~Ex: Student and Proctor Workstations must use the Test Delivery back end component to send messages to Monitoring and Alerting.~~ 3/8/2013 – Student and Proctor workstations will not utilize Monitoring and Alerting
~~RADMA.1.6~~	~~System Administrators will be able to delete M&A entries through a user interface based on age of the message and category (alerts, errors, metrics, logs) of the message. The user must be authorized to view the message to be able to delete it.~~	~~Framework~~	~~Medium~~	~~3/8/2013 – Based on discussions with David~~ Reqt removed after tech meeting discussion 4/8/13
~~RADMA.1.6.1~~	~~The user must be prompted to confirm that they intend to delete the data. "Alerts (metrics, errors, logs) prior to <date> will be deleted. Continue? Y,N"~~	~~Framework~~	~~Medium~~	Reqt removed after tech meeting discussion 4/8/13

RADMA.1.7	A timestamp will be applied to all message entities persisted by the component	Framework	High	
RADMA.2	Allow components to write log and tracing information in a consistent and configurable way.	Other	High	
RADMA.2.1	Allow components to write log and tracing information in a consistent way.	Framework	High	
RADMA.2.2	Allow components to write log and tracing information in a configurable way. All components should use a logging framework that is configurable outside of the component.	Configuration	Medium	Runtime configuration is limited to setting the logging level for an output source.
RADMA.3	Operational parameters are actively monitored – runtime metrics and dashboards.	Monitoring	High	
RADMA.3.1	Monitoring and Alerting will provide access to the metrics, errors and alerts raised by components through Monitoring and Alerting's user interface.	Dashboard	High	See Reqts. RFP.119.5, RFP.122, RADMA.1.2-3.
RADMA.4	Provide an API for collecting log information and alerts	Framework	High	
RADMA.4.1	Provide an API for collecting log, error, performance metric and alert information	Framework	High	Expansion of RADMA.4
RADMA.5	Provide the ability to expose information as to the status of a component	Dashboard	High	See RADMA.1.2
RADMA.5.1	Monitoring and Alerting will provide access to the status of a component through Monitoring and Alerting's user interface.	Dashboard	High	See RFP.88.1.4
RADMA.6	Provide the ability for machine or VM monitoring events experiencing low-memory issues, disk-full issues, processor overloading issues and exceptions to cause alerts which notify support personnel of possible issues. NOTE: the alerting urgency must be able to vary depending upon the availability category (High or Medium) for the component being monitored.	Monitoring	High	See RADMA.1.1
RADMA.6.1	Monitoring and Alerting must distinguish between High Urgency Alerts and Medium Urgency Alerts by an alert's severity level.	Monitoring	High	The urgency of the alert is determined by the component issuing the alert.
RADMA.7	Provide the ability to alert other components and possibly other vendor components accordingly.	Monitoring	High	
RADMA.7.1	The system must allow alerts to be sent to a specified group of clients.	Configuration	Medium	
RADMA.8	~~Provide an interface for all system components' log and alert messages.~~			Same as RADMA.4

RADMA.9	User interfaces for all components except for Reporting must support the following browsers at the indicated version and greater: ,,,,Internet Explorer 8+ (Windows) ,,,,Firefox 8+ (Macintosh, Linux & Windows) ,,,,Safari 5+ (Macintosh) ,,,,Chrome 16+ (Macintosh, Linux & Windows)			
PRMA.1	Provide a user interface for configuring alerts and rules that allow the component to make decisions based on the information collected from the other components of the system.	Configuration	High	
PRMA.1.1	A user interface will allow users with adequate permissions the ability to add/delete/edit rules of the form "If *(metric/alert)* has *(more/less/equal)* (*quantity)* occurrences in *(qty) (unit of time)* then create an alert *(alert description)* Ex: If "failed logons" has more than 50 occurrences in 5 minutes then create an alert "Possible security attack".	Configuration	Medium	This UI requirement is met by Hyperic's functionality. No custom UI will be needed since we are not using Monitoring and Alerting for workflow notifications.
PRMA.2	Provide a user interface capable of producing reports that indicate the overall health of the system, including performance metrics and error reports.	Reporting	High	
PRMA.2.1	~~The reporting features will be limited to those features provided by the selected off-the-shelf Monitoring and Alerting libraries. No additional customization to the package will be provided.~~	~~Reporting~~	~~High~~	
PRMA.2.2	The reporting features will use the centralized datastore for Metrics, Errors and Alerts and log messages.	Reporting	High	
PRMA.2.3	The User Interface for searching/viewing Monitoring and Alerting data must provide a "printable view" which allows user to print Monitoring and Alerting messages.	Reporting	High	Replaces PRMA.2.1
~~PRMA.2.4~~	~~The User Interface for searching/viewing Monitoring and Alerting data must allow search results to be exported to a .CSV file.~~	~~Reporting~~	~~High~~	Reqt removed after tech meeting discussion 4/8/13
PRMA.3	~~The monitoring and alerting component needs to provide capabilities to monitor server information as~~			Same as RADMA.5 and RADMA.6

	~~well as the software applications running on the servers.~~			
PRMA.4	The monitoring and alerting component will support a custom monitoring and alerting center. The system will be designed to receive information from a variety of sources, which might include ● third-party server monitoring software that monitors resource usage and raises alerts if resources approach critical levels ● internal event monitoring built into component systems.	Framework	High	See Reqts. : • PRMA.1 • RADMA.2 • RADMA.1.1 • RADMA.6
PRMA.5	The monitoring and alerting component will provide the ability for a component to report performance metrics, error logging, and workflow alerts	Framework	High	See Reqts: • RADMA.1 • RADMA.3 • RADMA.4.1
NFRMA.1	See Section 7 Non-Functional Requirements in the General Requirements document for up-time requirements as well as additional non-specific non-functional requirements..	Other	High	
NFRMA.2	Monitoring and Alerting, like most other identified components, is prescribed a minimum component server count of two (2) to maintain up-time requirements as well as accessibility in a single node failure. The architecture report was less prescriptive in the minimum data server count, specifying that it depends on application architecture.	Framework	High	
NFRMA.3	The Technical Proposal recommends that Monitoring and Alerting should be built upon a customized off the shelf commercial product~~. A competitive analysis cross matrix will be included as appendix A to the level II requirements document.~~	Other	Low	A comparison matrix is being created but will not be included in this document.
NFRMA.4	Infrastructure monitoring is a functional requirement, specifying, there must be ‘actionable’ items taken from the alert. The implied non-functional requirement is that when an alert is received regarding an infrastructure component nearing or exceeding an acceptable threshold that an administrator be provided the opportunity to provision more hardware. The actual means for such	Monitoring	Medium	See RFP.121

	provisioning will depend upon hosting solution chosen. However, a standard interface for taking action must be defined, the message must contain some amount of context and event identifier.			
NFRMA.5	~~XML is the format recommended by the Technical Proposal, with no mention of a required schema.~~	Framework	Low	The component will use JSON because it is quicker to parse, making it a better choice for a high-throughput component.
NFRMA.6	HTTP is the delivery protocol recommended by the Technical Proposal recommends with a presumably RESTful API.	Framework	Low	RESTful API's are being implemented.
NFRMA.7	As with all other components, it is required that Monitoring and Alerting be built with open-source technology, and the component be open sourced when completed.	Other	High	M&A is being built with open-source technology. DRC will deliver the component to AIR, who will open source the completed system.
NFRMA.8	Proper logging configuration guidance is an important deliverable for the Monitoring and Alerting, given that the component will responsible for keeping a centralized log for each component, it is highly important that the client components are logging only appropriate events to the Monitoring and Alerting component. This configuration can be controlled via the user interface listed above.	Configuration	Medium	See Reqts: • RFP.119.3 • RFP.119.4

VI. Data Transfer Listing

All components will provide data to the Monitoring and Alerting component. The following table describes the general API provided to every component.

Component Providing the Interface	Component Consuming the Interface	Input Data	Output Data	Data Format	Data Standard	Transfer Method	Notes/Description
Monitoring and Alerting	<Component>	Alert		XML/JSON		RESTful API	The <Component> component will send alerts to the Monitoring and Alerting component
Monitoring and Alerting	<Component>	Metric		XML/JSON		RESTful API	The <Component> component will send metrics to the Monitoring and Alerting component
~~Monitoring and Alerting~~	~~<Component>~~	~~Errors~~	-	~~XML/JSON~~	-	~~RESTful API~~	~~The <Component> component will send error messages to the Monitoring and Alerting component~~ Errors will be recorded through the logging API (3/20/13)
Monitoring and Alerting	<Component>	Logs			log4j		The <Component> component will send logging events to the Monitoring and Alerting component