NEXTIVA SMC SITUATION MANAGEMENT CENTER

1.01 GENERAL

A. All software components shall be part of the manufacturer’s standard software product offering.

B. All software components shall be thoroughly tested and proven in reference installations equal to or greater than the size and/or complexity of the Project.

C. Each systems integrator designing, proposing, implementing, supporting or otherwise participating in the maintenance, enhancement or upgrade of the PSIM solution shall hold factory certification on version being used or upgraded to by the end user.

D. The PSIM manufacturer shall offer the dealer/integrator/installer and end user access to a secure e-support website for Web-based technical information 24x7x365.

E. The PSIM manufacturer shall offer a variety of Service, Support plans and trainings.

1.02 PYSICAL SECURITY INFORMATION MANAGEMENT (PSIM) ARCHITECTURE

A. The PSIM shall use a flexible, open platform architecture built on accepted industry standards that facilitate integration with IT infrastructures.

B. The PSIM shall support running on COTS computer server, from a leading manufacturer (including IBM, Lenovo, Hewlett-Packard and Dell); with processors at minimum speed of 2.8 GHz from a leading manufacturer (including Intel or AMD); with a network-interface card with a minimum speed of 1GBPS. Hard-disk drive requirements should be identified during the system design preparations and be aligned accordingly.

C. The PSIM shall have a flexible, open architecture, and be able to migrate from a single site into a multisite system, e.g. components/servers comprised in the solution are deployable in a geographically disperse fashion.

D. The PSIM shall have a flexible, open architecture built on accepted industry standards that supports a Workgroup Microsoft Windows Environment.

E. The PSIM shall have a flexible, open architecture built on accepted industry standards that supports an Active Directory Domain Environment.

F. The PSIM shall support authentication with Windows user and password.

G. The PSIM shall be able to be installed in a Virtual Environment and be recognized by VMware as VMware Ready.

H. The PSIM shall offer redundancy solutions using the Marathon EverRun or VMWare ESXi platforms. Three possible solutions shall be supported:

1. The solution shall be redundant, using two separate servers, and achieve a fault tolerant, zero downtime environment and zero data loss.
2. The solution shall provide a disaster recovery option, using a third separate server at a secondary location which would assume primary responsibility in the event of a catastrophic event at the primary location.
3. The solution shall be redundant, using two separate servers, and achieve a high availability, minimal downtime environment. This design should not result in any data loss, however may require manual or automatic start of the application on the secondary server.

I. The PSIM shall possess an internal watchdog to detect and recover from the unlikely occurrence of a system lockup.

J. The PSIM Server component shall support software designed for the Microsoft® Windows® 2012 R2 (64 bit).

K. The PSIM Client component shall support Microsoft® Windows 7, or Windows 8 (32 or 64 bit) operating systems for workstations.

L. The PSIM shall be localization-ready and include support for Unicode characters, including double-byte and extended characters.

M. Scalability

N. Security

1.03 PSIM INTEGRATIONS

A. The PSIM shall support an unlimited number of integrated systems

B. The PSIM shall be an open architecture system allowing simple integration to external modules, sensors and systems, and allowing future scalability.

C. The PSIM shall be vendor agnostic and have the ability to interface with any type of security, safety or other business systems including, and not limited:

1. CCTV Surveillance Systems
2. Fire, Smoke and Gunshot Detection Systems
3. Panic button systems
4. Access Control Systems and Badging systems
5. Perimeter and Intruder Detection Systems
6. Face recognition/detection systems
7. License plate recognition systems
8. GPS tracking systems
9. CAD Systems
10. Crowd Sourcing
11. Mass Notification

1.04 PSIM CLIENT COMPONENTS

A. The PC workstation used to operate the PSIM clients application shall use equipment from a leading manufacturer (including IBM, Lenovo, Hewlett-Packard and Dell)

B. The system shall support multiple display, enabling drag and drop of modules to dedicated displays

C. System administration components

1. User management
2. Assets/Integrated system management

3. Health monitoring
4. Maps management
5. Response planning
6. Audit trails
7. Dispatch planning

D. PSIM operator Client

1. Supervisor Dashboard
2. Assets Monitoring
3. Video Surveillance
4. Alarm management
5. Incident management
6. Search
7. Reports

1.05 PSIM FUNCTIONS

A. User Management

1. The system shall support native authentication (e.g. against its own servers and stored credentials)
2. The system shall support authentication against Active Directory
3. The system shall simultaneously support both authentication types
4. The system shall have the ability to order users in hierarchal groups structure
5. The system shall have the ability of disabling\enabling existing user account without deleting it
6. The system shall allow capturing user's data (include name, e-mail and phone number) as part of the user account creation.
7. The system shall provide for the definitions of roles where each role has a set of configurable privileges
8. The system should group privileges based on modules and functionality areas and allow multi selection of all privileges in a group.
9. The system shall have the ability to assign a role to a user and define the devices scope that this role applies to
10. The system shall have the ability to effectively assign multiple sets of privileges on multiple sets of resources/devices to a single user

B. Integrated systems management (assets)

1. The system shall allow managing integrations servers from a central administration application
2. The system shall support multiple integrations servers working with the same application and database servers

3. The system shall allow configuring system adaptors in integration server from a central administration application
4. The system shall allow configuring the system adaptor connection information (IP, user, password) from a central administration application
5. The system shall allow discovering the devices of the integrated system and allow the administrator to define/select which devices should be monitored by the system
6. The system shall allow viewing the discovered device in a list and enable sorting of that list based on device type, name, monitoring state.
7. The system shall allow selective monitoring of subset of all available devices of a specific integrated system
8. The system shall allow assigning a display name and a description for the integrated device
9. The system shall allow ordering the monitored devices in a multi-level tree structure that represents the organizations operation hierarchy
10. The system shall show icon, next to each device entry, that represents the device type
11. The system shall allow filtering the monitored devices tree by device type
12. The system shall allow searching the monitored devices tree by device name
13. The system shall allow creating relationships between devices of same or different systems. These relationships shall be used for automation, accessibility, etc.
14. The system shall allow creating relationships between a device and a PTZ camera and specific preset
15. The system shall monitor and ensure that enabled system adaptors are up and running
16. The system shall support purging of alarms/incident data records according to administrator parameter setting

C. Health Monitoring

1. The system shall allow viewing health monitoring data in a dashboard layout
2. The system shall support health monitoring of both physical servers and system components (e.g. services, plug-ins) including CPU/Memory/Disk utilization and network connectivity performance
3. The system shall present the different components status using standard color codes showing the health of each component, along with the system administrative alerts list
4. The system shall present health status based on hardware indicators
5. The system shall present administrative alerts based on system operative events (e.g. mail server not reachable, devices offline)

6. The system shall support drill down capability for presenting actual alerts per selected component
7. The system shall support thresholds settings per each monitored server

D. Maps management

1. The system shall allow definition of multiple maps
2. The system shall allow ordering the maps in a hierarchal tree structure
3. The system shall allow adding multiple layers to a map
4. The system shall provide the maps administrator with a feature-rich map control and browsing capabilities including geo-coding and reverse geo-coding
5. The system shall allow adding layers from service sources including Open Street Map, ArcGIS online and ArcGIS servers
6. The system shall allow adding layers from registered file formats as well as unregistered file formats
7. The system shall allow having online service layers and local files layers on the same map
8. The system shall allow ordering the layers in a hierarchal tree structure
9. The system shall allow adding monitored devices layers and place devices on them
10. The system shall enable searching for a device by name or type in order to select if for placing
11. The system shall allow interacting with the device (play video for cameras, close relays) from the map management module
12. The system shall allow removing a device from a specific layer
13. The system shall allow editing device's GIS location by locating it on the map or by inputting its exact GIS coordinates
14. The system shall allow viewing the layer that the device is included in from the device icon on the map
15. The system shall save the map context (extent, layers selection) when browsing between maps
16. The system shall allow defining kick-in and kick-out zoom levels per layer. Such customization will allow showing layers of different details level at the right context.
17. The system shall allow defining cameras and devices coverage area. Coverage area should include coverage area range, angle and orientation.
18. The system shall display device coverage area as a semitransparent polygon on the map.
19. The system shall allow showing\hiding the coverage area for a single or all devices.

20. The system shall allow adding point of interest markers that can also include links to other maps and will be used as on-map hyperlinks.
21. The system shall enable administrator to grant privileges to manage maps and\or place devices.

E. Incident response planning

1. The system shall allow management (Add, delete, modify and rename) of incident types
2. The system shall support management of response procedures
3. The system shall support adding to-do tasks in the response procedures
4. The system shall support adding decision tasks with multiple options in the response procedures
5. The system shall support adding manually initiated device command tasks in the response procedures. Device command tasks should include sending camera to preset, control doors, dispatch, etc.
6. The system shall allow selecting which device to apply the command to. Automatic device selection (based on event that triggered the incident) or manual selection should be supported.
7. The system shall support adding automatically initiated system command tasks in the response procedures. System command tasks should include sending e-mail.
8. The system shall support automatic initiation of device and system commands upon incident creation.
9. The system shall enable associating response procedures to incident types. The associated procedures should be available for selection to operators upon manual incident creation.
10. The system shall allow configuring and executing incident triggering rules
11. The system shall allow setting up multiple triggering rules per incident type
12. The system shall allow setting up rules with complex triggering conditions, including multiple occurrences of an event within a timeframe and dependencies between occurrences of events
13. The system shall allow enabling\disabling rules and this change should take effect on the fly
14. Incident triggering rules should include conditions referring to the following data event details: event type equals to, event sub type equals to, event source device is included in, event description contains.
15. The system shall enable setting the severity and the response procedure that will be associated with the automatically triggered incident
16. The system shall allow adding dispatch commands as part of the response procedures

F. Audit trails

1. The system shall retain/store all user activity audit records
2. The system shall provide an application for searching these records

3. The system shall provide audit record search capability based on time, user name, user full name, action description and IP address
4. The system shall display audit records search results in a tabular structure that supports sorting, grouping and searching within results
5. The system shall allow exporting the audit search results into a tabular file format (e.g. XML)

G. Dispatch Incident (In addition, place holder for NowForce A&E link)

1. The system shall allow mapping incident/mission dispatch
2. The system shall allow different dispatch missions based on incident severity
3. The system shall allow automatic system initiated dispatch request
4. The system shall allow manual operator initiated dispatch request
5. The system shall report upon successful dispatch request
6. The system shall allow request of mission abort
7. The system shall update the incident record on all dispatch system reports including dispatch ongoing status, responders allocation and ongoing mission handling reports
8. The system shall support responders initiated alarms (e.g. panic alarm)
9. The system shall allow manual dispatch of responders to an active incident
10. The system shall automatically close the dispatch mission upon closure from all responders and fulfillment of the dispatch rule
11. The system shall validate completion of an active dispatch upon incident closure

H. Supervisor Dashboard

1. The system shall provide supervisors with a KPI driven dashboard that measures the performance of the control room
2. The dashboard should include performance visualization related to alarm handling and follow alarm response time KPI, number of active alarms
3. The dashboard should include performance visualization related to incident handling and follow average incident response time KPI, active incident resolution time KPI
4. The dashboard should include counters and graphs displaying number of alarms and incidents and also by severity and by type distribution graphs
5. The dashboard should include a map for laying out the information geographically. User should be able to set the map and its extent.
6. The dashboard should allow drilling down to the relevant module (alarms or incidents) from a specific graph\gauge.
7. The system shall allow administrators and/or Supervisor to setup the customer specific KPI numbers
8. The system shall allow the user to order the dashboard components

I. Assets monitoring

1. The system should present the operator with a logical tree that contains devices from different types
2. The system should enforce that each operator sees only the defined device scope
3. The system shall allow searching the device tree by device name or device type
4. The system shall indicate the device type by an icon
5. The system shall allow sending commands to a device from its tree entry or its map icon. Sending commands privilege should be configurable as part of the user role.
6. The system should display the related devices for the selected device.
7. The system should display the devices on maps as icons that correspond to the device type
8. The system should display a pop-up for a device with its details
9. The system should allow zooming the map to a device location from the device entry in the tree
10. The system shall update the maps of all logged in operators with location change that is received from GPS tracked devices
11. The system shall display an icon for each device that is placed on map
12. The assets map should allow pan, zoom, and rotation via standard mouse operations (e.g. wheel for zoom-in\out) and on map control.
13. The system shall enable to operator to show\hide background or devices layers
14. The system shall cluster devices whose icons overlap so that the map is not cluttered when zooming out.
15. The system shall allow operator to set the device icons clustering sensitivity.
16. The system shall allow operators to show\hide devices coverage area
17. The system shall allow operators to request to see live video from cameras whose coverage area is covering a point on the map selected by the operator
18. The system shall support playing live video for cameras or for devices that has related camera
19. The system shall support geo-association; Pinning an area of interest on the Map and as a result, automatically showing all the devices which have coverage on the pinned area and for the relevant camera devices, play live video

J. **Video Workspace** (in case of a third party VMS. Refer to Nextiva VMS A&E specifications document in case of Nextiva VMS)

1. The system shall have a video viewing graphical user interface (GUI) that allows users to view live video, retrieve recorded video
2. The system Video workspace shall enable users to manage multiple tabs and perform multiple tasks simultaneously. It should include the following functionality:

    i. Hot function keys (show hide tree, quick query – live/recorded)

    ii. Configurable playback speed in multiple increments up to x16
    iii. The ability to view live or recorded video in multiple tiles, including video from multiple Digital Video Recorders and multiple sites
    iv. Variable speed PTZ camera control (camera dependent)
    v. The ability to take-over a PTZ function, depending on user rights and priority levels
    vi. Support for camera presets (go to preset, not define preset)
    vii. Support ImmerVision (360 degree panoramic lens) camera viewing
    viii. Allow to designate an object and to view all cameras overseeing the object in their field of view

3. The system shall allow the user to open, move, and size multiple, independent video tiles as needed, including:
    - i. Single windows
    - ii. 2 x 2: 4 (quad) windows, arranged in two rows of two windows each
    - iii. 5 x1 window, arranged in one large window, surrounded by multiple tiles
    - iv. 3 x 3: 9 windows, arranged in three rows of three windows each
    - v. 4 x 4: 16 windows, arranged in four rows of four windows each
4. The system shall allow the user to view and work independently in 4 different tabs including:
    - i. default
    - ii. alarms
    - iii. incidents
    - iv. designation/geo-relation
5. The system shall support digital zoom on live or recorded video, without requiring a video pause
6. The system shall enable/disable video de-interlacing
7. The system shall enable users to request video from a camera at a specified date and time, and for a specified duration (duration in preferences)
8. The system shall support drag-and-drop camera selection from the camera tree and between tiles
9. The system shall support attaching video/snapshot to incident from any camera , tile and mode (live/recorded)
10. The system shall support video request processing.
11. The system shall support video playback controls, including:
    - i. Buttons to start and stop playback from the current video position
    - ii. Button for moving through video in reverse
    - iii. Positioning controls, including a slider bar and buttons to quickly and conveniently position to the beginning, end, or any other time in the video clip

12. The system shall support camera presets by providing a toolbar, or other GUI method, for working with camera presets when viewing live video from a PTZ camera.

13. Video workspace operations shall be able to be restricted. It shall be possible to restrict or enable the following functionality:

    i. Live video

    ii. PTZ control

    iii. Recorded video

K. Alarm management

1. The system shall display all alarms in a unified grid

2. The system shall support sorting and filtering of the alarms grid based on every displayed column

3. The system shall support text based searching in the alarms grid

4. The system shall visually notify operators upon receiving new alarms in a non-blocking manner. The visual notifications can be turned on\off per operator's preference.

5. The system shall allow clearing alarms. Cleared alarm should be visually different from active alarms.

6. The system should update the alarm record on all operators workstations when an operator clears an alarm

7. The system should log and display the time and the user name of the operator that cleared the alarm

8. The system should display the alarm details upon alarm selection. Details should include source device and its related devices, alarm meta data, alarm attached images.

9. The system shall allow zooming in on the alarm location

10. The system shall allow viewing recorded video from the time of the alarm. System should deduce the relevant camera based on the alarmed device and its related cameras.

11. The system shall enable opening all alarm-related video (live and recorded) in the video workspace

12. The system should display the alarm record, its details, its location and related video in a single screen

L. The system shall support drill in capabilities for alarm; automatic and/or manualy requesting and presenting extended information from integrated systems based on the alarm data.

M. Incident management

1. The system shall display all active incidents in a unified list

2. The system shall support sorting and filtering of the incident list based on every displayed column

3. The system shall visually and audibly notify operators upon receiving new incidents. The visual notifications can be turned on\off per operator's preference.

4. The system shall update the incident record on all operators workstation for any activity done by the operator on the incident ensuring consistent common operational picture
5. The system shall allow creation of new incident with/without geographical context
6. The system shall allow the user to set the type, severity, description, time, response procedure of the manually created incident.
7. The system shall capture as much information from the new incident creation context and populate it to the incident (time, description, location).
8. The system shall allow the user that creates incident to auto assign it to him\her.
9. The system shall allow taking ownership of unhandled incidents. This action should be managed by a dedicated privilege.
10. The system shall allow taking ownership of a handled incident in accordance to the organization hierarchy and privileges.
11. The system shall allow the incident owner to indicate escalation status of the incident
12. The system shall support automatic escalation of an incident by monitoring and visually indicating escalation of incidents according to defined KPIs
13. The system should log and display the time and the user name of the operator that accepted the incident
14. The system shall allow editing the incident severity, timestamp and description. Upon editing incident severity, user that is viewing this incident should get visual notification that the severity was changed.
15. The system shall allow setting and changing incident location
16. The system shall allow the owning user to close the incident
17. The system shall suggest the user to add incident summary upon incident closure
18. The system shall allow exporting an incident summary report in pdf format, saving and viewing it. The incident summary report should include the incident details, attachments and their image preview, chronological activity timeline with the main incident lifecycle information.
19. The system should display the incident details upon incident selection. Details should include relevant response plan, logged activities performed on the incident, attachments (including source alarm) and incident source device and its related devices.
20. The system shall allow zooming in on the incident map location. The selected incident map icon should be highlighted.
21. The system shall include full map capabilities in the context of the incident where user can select map, layers, interact with on-map items, etc.
22. The system shall allow viewing recorded video from the time of the incident. The system should deduce the relevant camera based on the alarmed device and its related cameras.

23. The system shall enable opening all incident related video (live and recorded) in the video workspace. Recorded and live video from the same camera should be displayed side by side.

24. The system should display the incident record, its details, its location and related video in a single screen

25. The system shall allow attaching map & video snapshots to the incident

26. The system shall allow attaching video tags to the incident

27. The system shall allow viewing incident attachments including maps and video snapshot in its default viewer. In case of video tags, the system shall allow viewing the tagged video in the video workspace

28. The system shall allow attaching\removing events/alarms to an incident

29. The system shall allow viewing incident attached alarms details. Details should include source device and its related devices, alarm meta data, alarm attached images.

30. The system shall allow zooming in on the attached alarms location and playback of alarm related video

31. The system shall allow adding comments to the incident. Each comments shall be logged with the operator user name and the comments time stamp

32. The system shall allow operator to execute the incident response plan

33. The system shall display for each of the response plan tasks its description

34. The system shall log all response plan tasks executed by the operator

35. The system shall present response plan execution overall progress

36. In case of decision point tasks, the system shall allow the operator to review the different optional routes before taking the decision

37. In case of command tasks, the system shall allow operator to continue working while command is being executed

38. The system shall support multitasking between incidents. When browsing between incidents, the incident form state (map, video, selections) should be persisted so the user will continue operation from same place.

39. The system shall allocate a video workspace per incident so videos not related to that specific incident tasks (e.g. routine monitoring, alarm assessment) will not be mixed.

40. The system shall persist the video workspace of the incident when multitasking between incidents so user will not lose the video context when browsing between incidents.

41. The system shall support incident response collaboration between multiple operators. Multiple operators should be able to mark tasks as done, add comments, and add attachments to the incident. Every change in the incident should be populated across all workstations.

42. The system shall enforce that operators are getting visibility for incidents based on their visibility to the device that triggered the incident.

43. The system shall enable visibility for incidents that are not associated with a device based on the defined organizational tree hierarchy. Colleague users in the same group and users higher in the hierarchy of the incident creating user should gain visibility to that manually created incident.

N. Search

1. The system shall provide search capabilities on all event, alarms and incident records
2. The system shall provide Incident record search capability based on Incident ID, type, description, time and severity
3. The system shall display incident records search results in a tabular structure that supports sorting, searching within results
4. The system shall allow viewing selected incidents details
5. The system shall allow exporting the Incident search results into a tabular file format (e.g. CSV)
6. The system shall provide events record search capability based on event type, sub type, time and severity and source devices
7. Based on the event type, the system shall provide type specific custom fields as search parameters
8. The system shall allow partial search using wildcard on the event custom fields
9. The system shall display events records search results in a tabular structure that supports sorting, searching within results
10. The system shall allow creating new incidents from the event record
11. The system shall allow attaching of an event record to an active incident
12. The system shall allow exporting the events search results into a tabular file format (e.g. CSV)

O. Reporting

1. The system shall provide privilege-based reporting capabilities
2. The system shall provide operational reports on incidents based on user defined timeframe
3. The system shall provide statistical reports on incidents and alarms
4. The system shall provide trend reports on alarms

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited. By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change.

Verint Systems Inc. does not warrant, guarantee or make any representation regarding the use or the results of the use of the information, links, tools, and materials in terms of the accuracy, reliability, quality, validity, stability, completeness, currentness, or otherwise of its content or products. The entire risk as to the use, results and performance of information, links, tools and materials provided or referenced herein is assumed by the user. Verint Systems Inc. shall not be liable for damages resulting from the use, misuse or unlawful use of the information, links, tools, and materials contained or referenced herein.

The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,689,442; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,724,887; USPN 6,751,297; USPN 6,757,361; USPN 6,782,093; USPN 6,952,732; USPN 6,959,078; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 7,216,162; USPN 7,219,138; USPN 7,254,546; USPN 7,281,173; USPN 7,284,049; USPN 7,325,190; USPN 7,424,715; USPN 7,466,816; USPN 7,478,051; USPN RE40,634; and other provisional rights from one or more of the following Published US Patent Applications: US 11/394,408; US 11/771,499; US 11/396,514; US 11/772,440; US 11/565,943; US 11/565,946; US 11/565,948; US 11/540,739; US 11/540,086; US 11/541,313; US 11/541,252; US 11/540,282; US 11/529,947; US 11/540,785; US 11/540,736; US 11/540,904; US 11/540,353; US 11/608,340; US 11/608,350; US 11/608,358; US 11/567,808; US 11/692,983; US 11/693,933; US 11/693,923; US 11/693,828; US 11/567,852; US 11/608,440; US 12/015,621; US 11/540,322; US 11/924,201; US 11/616,490; US 11/621,134; US 11/752,458; US 11/712,933; US 11/824,980; US 11/729,185; US 11/804,748; US 11/831,260; US 11/395,992; US 11/359,319; US 11/359,195; US 11/359,357; US 10/832,509; US 11/742,733; US 11/831,257; US 11/831,250; US 11/691,530; US 11/479,267; US 11/529,942; US 11/768,349; US 11/540,281; US 10/633,357; US 11/693,899; US 11/479,056; US 11/529,132; US 11/540,320; US 11/037,604; US 11/529,842; US 11/540,171; US 11/478,714; US 11/529,946; US 11/868,656; US 11/776,659; US 11/090,638; US 11/410,004; US 10/771,315; US 10/771,409; US 11/540,900; US 11/528,267; US 12/118,781; and other U.S. and International Patents and Patents Pending.

VERINT, the VERINT logo, ACTIONABLE INTELLIGENCE, POWERING ACTIONABLE INTELLIGENCE, WITNESS ACTIONABLE SOLUTIONS, STAR-GATE, RELIANT, VANTAGE, X-TRACT, NEXTIVA, ULTRA, AUDIOLOG, WITNESS, the WITNESS logo, IMPACT 360, the IMPACT 360 logo, IMPROVE EVERYTHING, EQUALITY, CONTACTSTORE, and CLICK2STAFF are trademarks or registered trademarks of Verint Systems Inc. or its subsidiaries. Other trademarks mentioned are the property of their respective owners.