1.1.1 SYSTEM TECHNICAL REQUIREMENTS
Shall address all of the following:
a) Incident investigations and workflow
b) Forensics support
c) Security and compliance reporting and visualizations
d) Real time monitoring and alerting on both known and unknown threats
e) Cross-data source correlations to detect specific patterns
f) Full text search of all ingested data using pattern matching and regular expressions
g) Long-term metadata retention
1. Scalable architecture capable of supporting customer deployments with the following parameters:
i. Able to scale horizontally

ii. All data shall be searchable immediately after indexing
iii. Data shall be retained and stored local to each site in which it was collected
iv. Able to correlate data from distributed collections points
v. Ability to index all the original, unmodified metadata and make it searchable and reportable (no data normalization or data loss)
vi. Scale out on hardware with no fixed limit on storage (add more hardware as needed)
2. The systems shall collect metadata for layer 4 and layer 7 flow information which provide in-depth packet payload information for additional insight in network traffic and events.
i. Shall handle timestamps from different time zones
ii. Shall handle sub-second resolution on timestamps
3. The systems shall be able to process metadata for a minimum of 1,200,000 network flows per minute per instance.
4. The systems shall be able to process metadata for a minimum of 20,000 events per second per instance.
5. The systems shall be able to process metadata for layer 7 flows up to 10 gigabit per second per device.
6. The systems shall have network behavior analysis functionality to identify any anomaly or unknown attack/traffic that may exist in the network and provide alerts or reports for ease in quick reaction.

7.	The systems shall perform de-duplication at the collector to display a single event at the console.
8.	The systems shall be able to immediately handle metadata for 60,000 events per second at each location. Proposed architecture without major modification shall be scalable to 120,000 events per second.
9.	The systems shall have sufficient local storage to hold up to 1 years' worth of metadata required by the proposed solution at each location.
i.	Storage should be handled in a 2 tier manner allowing high speed access to data stored within the past 90 days and a second tier of storage for the remainder of the data
ii.	Resources to provide data backups for the solution, data backup solution cannot require hand-on maintenance
iii.	Backup solution shall encompass full system backups, as well as data backups for all tier 1 and tier 2 storage
iv.	Onsite backups shall; be redundant, have granularly configurable frequency and scope, include system configurations and protected against SIEM failure of any kind. (i.e. power failure, media failure, data corruption, etc)
v.	Storage shall include a "non-returnable" disk provision in compliance with VA Handbook 6500.
vi.	Ability for replication of data to maintain multiple, identical copies of data for availability, fidelity, disaster recovery, and improved search performance
10.	The systems shall be fault tolerant, provide High Availability at each site.
i.	Advanced remote management for all components in the converged infrastructure shall be included
ii.	All components of the converged infrastructure shall provide resiliency in case of component failure.

11.	The master console shall provide High Availability locally as well as provide disaster recovery between Hines, IL and Martinsburg, WV.
12.	The systems shall provide role-based access control (RBAC) to restrict access to views based on user's role.
13.	The systems shall create a detailed, non-modifiable log for operating system, application, administrator, and user activity to ensure proper accountability for the system.
14.	The systems shall not allow shared accounts for configuration and administration of the vendor's product.
15.	The systems shall store all passwords in an encrypted format and not display passwords on logon screens in clear text.
16.	The systems shall force users to logoff after a configurable period of time.
17.	The systems shall provide security controls and audit ability as required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53r4 and VA-Handbook 6500 for a high risk system.
18.	The systems shall provide an encrypted (Transport Layer Security (TLS) 2.0 or better) for all web accessible interfaces.
19.	The systems shall use https/Secure Socket Layer (SSL) connections for any web-based access. The systems should support customer provided SSL certificates, signed by an internal, customer hosted certificate authority. The solution should support a private key with a minimum of 2048 bits.
20.	Two ZeroU vertical switched rack mount PDUs per rack i. Fit in a standard 42 U rack (if one is not proposed with the solution) ii. Capability to manage the power ports (on / off) over IP as well as console connection. iii. Capability to manage (access, configure) via web (https) and SSH iv. Shall have a Load indicator LED v. Shall be compatible with APC Centralized Management platform using InfraStructure Central vi. Output: Output Voltage: 200V, 208V Output Connections: At least 3 IEC 320 C19 outlets (or compatible outlets that meets powering the hardware unit(s) proposed). In addition, additional outlets to meet powering the proposed solution. vii. Input: Input voltage: 208V, three phase

- Input connections: NEMA L6-30P

21. The systems shall provide all network connectivity, including cabling and small form-factor pluggable (SFPs) if needed, to attach to existing 10 gigabit fiber ports or to existing 1 gigabit copper ports on the Cisco Nexus 7000 in the TIC Gateways, and to existing switch equipment in all other locations.

22. Each system's hardware shall be installed in one (1) equipment rack of no more than forty-two (42) rack units (RUs). Systems shall be limited to one (1) rack per TIC and Lab location.
    i. i.e. The VA only has room for the SIEM to occupy one (1) standard 42 RU rack in each of the TIC locations with the Lab as a perfect replica of the configuration in one of the TICs.
23. The solution shall not exceed 15,000 BTU per hour in each TIC location.
24. Console equipment shall not exceed four (4) Rack Units (RUs)

1.1.2 EVENT COLLECTION REQUIREMENTS

1. The systems shall have the ability to set notification timeframes/ schedules based on priority and classification of events and correlated of events.
2. The top level instance(s) shall have access to these correlated events as well as the ability to configure unique specific events as well as configurable single events for correlation across all instances.
3. The systems shall report new (i.e. not in the existing inventory) network elements as a notifiable event.
4. The systems shall identify and store baseline performance attributes.
5. The systems shall allow users to adjust thresholds for each element being monitored.
6. The systems shall allow multiple thresholds per element to define warning and critical levels.
7. The systems shall identify when an element exceeds a threshold.
8. The systems shall allow elements to be put into a maintenance state to suppress alarms from the element.
9. The systems shall provide date/time stamp and identify source of all event data collected and store it in repository.
10. The systems shall maintain a query-able repository of all network devices and event data elements monitored.
11. The systems shall be capable of collecting events from network infrastructure devices (i.e., firewalls, IPS devices, application layer security solutions, antivirus solutions, routers, host-based intrusion prevention systems, operating systems, etc.) in accordance

with the VA TRM.
12. The systems shall include a configurable development kit for custom event collectors.
13. Shall be able to leverage external data sources to enrich events, add context, and create more specific correlation searches
i. Employee information (e.g., Active Directory/LDAP)
ii. Asset information (e.g., hostname, IP address, system function, system owner, etc.)
iii. Lists of prohibited services/processes/IPs/ports/protocols
iv. Ability to add new threat intelligence feeds, whether open-source or proprietary
v. Other arbitrary lists (e.g. usernames or email addresses)
14. Support for the following log data sources:
i. Palo Alto Firewalls
ii. Cisco IronPort
iii. Cisco Network Access Control
iv. Cisco Access Control System
v. Cisco IOS
vi. Cisco ASA Firewalls
vii. Cisco ASA VPN
viii. IBM ISS IPS
ix. SourceFire Defense Center
x. F5 Application Security Module
xi. F5 DNS Logs
xii. F5 Global Traffic Manager
xiii. Citrix Netscaler
xiv. UNIX Authentication Logs
xv. Windows Authentication Logs

xvi. Netapp Filer
xvii. McAfee EPO
xviii. IBM Endpoint Manager
xix. Network Flows (NetFlow, IPFIX, etc)
xx. PCAP files
xxi. Hosted VM environments (Amazon Web Services, Rackspace, etc)
xxii. Cloud-based applications (Box, Salesforce.com, etc)
xxiii. Social media (Twitter, Facebook, Foursquare, etc)
1.1.3 AUTOMATED ACTION REQUIREMENTS
1. The systems shall provide configurable event conditions (e.g. by type of event, by element or sub-element, by user-defined group, by time of day, by day of week).
2. The systems shall automatically provide configurable notification of events to network and non-network devices.
3. The systems shall provide the ability to selectively create a VA Remedy and/or CA UniCenter trouble tickets.
4. The systems shall provide user configurable and built-in rules to determine the root cause of problems in the network.
5. The systems shall provide configurable rules so that devices and conditions can be added, changed, or removed.
6. The systems shall analyze fault data to form a conclusion that determines a root cause and/or assist the user in determining a root cause.
7. The systems shall analyze threshold event data to determine what constitutes normal (baselining).
8. The systems shall correlate several events from disparate systems into a single, meta-event.
9. The systems shall aggregate several events from the same system into user configurable thresholds.
10. The systems shall receive events with the capability to be fielded, filtered, and sorted.

11. The systems shall factor in thresholds while integrating and correlating events.
12. The systems shall have the ability to retrieve inventory and other event data from external event data repositories so that the event data can be used to enrich the analysis of events.
13. The systems shall have the ability to correlate event data based upon network based indicators from disparate systems to identify and alert upon security based policies designed to identify malicious activity on the network.
14. The systems shall have the ability to do event data mining for analysis.
15. The systems shall have the ability to export event data.
1.1.4 REPORTING REQUIREMENTS
1. The systems shall allow users to use built-in and custom reports.
2. The systems shall generate analysis reports that use both historical as well as real-time event data.
3. The systems shall maintain a repository of historical events that can be easily accessed via external applications.
4. Reports and dashboards can be modified
5. Reports and dashboards support drill-down capabilities to get from a high-level dashboard to a raw event
6. Offers an industry standard application program interface (API)(REST/SOAP/XMLRPC/etc) to expose all data, search and functionality to external systems, applications or dashboards