Attachment 001
Securing Medical Devices and Internet of Things (IoT)
MedFusion Pilot Concept Document

1. Pilot Solution Requirements

The MEDFUSION pilot shall validate a solution to meet the intent of reducing cyber security material weakness without creating an overly complex environment and by maximizing re-use of existing infrastructure. A balance of operational ability and security shall be attained to meet the VA's dynamic environmental and mission requirements. This requires that the Integrator of the pilot solution be able to demonstrate number seamless operational requirements including the ability to demonstrate an agentless network discovery of Open Systems Interconnection (OSI) Layer 2/3 devices that are able to discover and authenticate authorized wired, wireless, Virtual Private Network (VPN) or Bring Your Own Device (BYOD) end-point devices (based on industry and vendor defined characteristics). The pilot network overhead shall be unobtrusive (or negligible) to network performance. In addition, the pilot needs to interface with existing VA discovery Continuous Diagnostics Monitoring (CDM) products such as Gigamon. The pilot solution hardware and software) must integrate with existing Network Security Operations Center (NSOC) Unified Computing Service (UCS), which is comprised of a Cisco management platform consisting of Cisco Firepower, Cisco ISE, Cisco behavioral analytics Stealthwatch, and must natively integrate with vulnerability platform Tenable Nessus. It must also natively interface with existing Enterprise Security Splunk. It is required the pilot employ the use of Cisco Next-Generation Intrusion Prevention System (NGIPS) & Next-Generation Firewall (NGFW). The pilot shall be capable of reporting many facets of the Enterprise ecosystem including inventory, timestamped entry/exit behavior of devices, usability, alerts for additional segmentation needs, (intranet) peer-to-peer traffic analysis. The pilot solution provide heuristic insight of the network through a layer-7 dashboard modifiable presentation whose consumption of near-real time analytics make it effective for consumption of data from the C-Level to the bio-medical support community and to the specialized Information Technology (IT) specialist for any required remediation efforts. An analogy would be that VA requires the use of a holistic 'single-pane-of-glass' dashboard that aggregates a multitude suite of tools.

The Contractors solution shall:

- Leverage next-generation identity device and access control policy appliances with enhanced network switch port access control mechanisms to enable automated device discovery and automated Layer 3 network access control.
- Integrate security monitoring and event reporting capabilities to provide near real-time alerting and correlation.
- Provide malware identification and management to include the use of next generation firewalls and intrusion prevention appliances which enable 'deep-packet' layer 3-7 inspection of all network traffic and the quarantine and remediation of suspicious packets.

The MEDFUSION Pilot shall demonstrate a comprehensive network security control solution that encompasses the following key capabilities:

Endpoint Isolation –The solution shall provide a comprehensive method of selectively isolating the devices on the network and ensure that connectivity is strictly limited to those communication paths that are required for a given device to function properly and nothing more. The medical and special purpose devices shall be protected from other devices on both the internal and external networks. Conversely, other devices on the internal networks will similarly be protected from the medical and special purpose devices.

Threat Management/Anomaly Detection – It is required that the rapid detection and management of network threats via a variety of methods, including Intrusion Prevention System (IPS)/signature based detection, file analysis, statistical based network monitoring, anomaly detection with configurable thresholds and dynamic response based on policy. All of these methods shall be used in any situation in order to detect all possible types of threats, including zero-day attacks.

Configuration Management – Effective, centralized management of the network security architecture which reduces the risk of misconfiguration and unauthorized modification of security policies.

Discovery, Network Access Control, Asset Management – The solution shall provide for rapid device discovery and asset management. Medical and special purpose devices shall be detected the moment they are connected to the network and assigned the proper security policies based on their unique device characteristics. Unknown devices shall be automatically segregated into isolation enclaves to allow for subsequent analysis and categorization. Asset management capabilities shall be integrated with this process so that at any given instant in time, all devices active on the network can be identified.

Continuous Monitoring – The solution shall provide a single, integrated, robust security event collection and correlation mechanism for monitoring all of the security events from all of the critical devices. This mechanism shall provide near real-time monitoring of security events throughout the enterprise along with the ability to report on historical trends of all of the security events. Additional ability to correlate events received from varying security event sources is required in order to enable effective root cause and impact analysis.

1.1. Other Requirements and Constraints

1. Special Purpose Systems/Medical Devices (SPS/MDs) cannot have software installed. The solution shall be agentless.
2. SPS/MDs communicate via IPv4 and/or IPv6 and may connect to the VA network in a variety of ways (e.g., single or multiple 10/100/1000Mbps Ethernet or 10Gbps Ethernet NICs, Wifi, etc.).
3. SPS/MDs may or may not be on the same broadcast domain as other SPS/MDs and non SPS/MDs.

4. The solution shall have the ability to scale indefinitely (i.e., scale to millions of SPS/MDs).
5. The solution shall take into account the large variety of environments within the VA (local, region, enterprise) in which SPS/MDs may be found. Environments differ in physical characteristics, high availability requirements, and criticality. The solution will not require changing VA's production layer 2 or above topology.
6. A variety of networking technologies may be in use by SPS/MDs and shall be accounted for (e.g. QoS, 802.1q, 802.1ad link aggregation, event log export, device integrity enforcement, encryption, endpoint security solutions).
7. The solution shall take advantage of current VA systems (e.g., routers, switches, firewalls, etc.) and shall integrate with VA management systems (e.g., Security Information and Event Management (SIEM), Active Directory, Simple Network Management Protocol (SNMP)).
8. Factor: Latency shall be considered. Some SPS/MDs may be heavily latency sensitive while others may not be.
9. Solution lifecycle management shall be considered, to include centralized management. Due to the scope of the initiative, the solution shall maximize automated services, as-well-as granular system tuning to avoid false positives.
10. The solution shall provide logical isolation of the SPS/MD from other SPS/MDs as well as non SPS/MDs for the purpose of protecting both the SPS/MD as well as the VA network. While the VA is seeking industry input regarding the level of isolation needed, the full range of modern attack vectors shall be addressed covering all layers of the OSI model, including modern and trending threats such as Advanced Persistent Threat (APT) and zero-day attacks. Integration with and reporting to outside entities (e.g., Medical Device Innovation Safety and Security Consortium, etc.) shall be considered.
11. Solution shall be able to provide both general and detailed reporting of a variety of SPS/MD characteristics (e.g., traffic volume, ports and protocols in use, threat indicators, and in the case of Bio-Med, the use of equipment category and model serve as fields most relevant to track and manage to identify the devices).
12. Solution shall address unknown SPS/MD discovery methodology as well as cataloging of all known SPS/MDs.
13. The solution shall be extensible and not reliant on proprietary protocols or methodologies.
14. The solution shall conform to all applicable laws, regulations, and VA 6500 series Directives and Handbook standards.
15. The solution shall support WIFI communication security to prevent eavesdropping on the channel(s).
16. Change Management – Configuration files (and event logs) must be and available for exportable for storage.

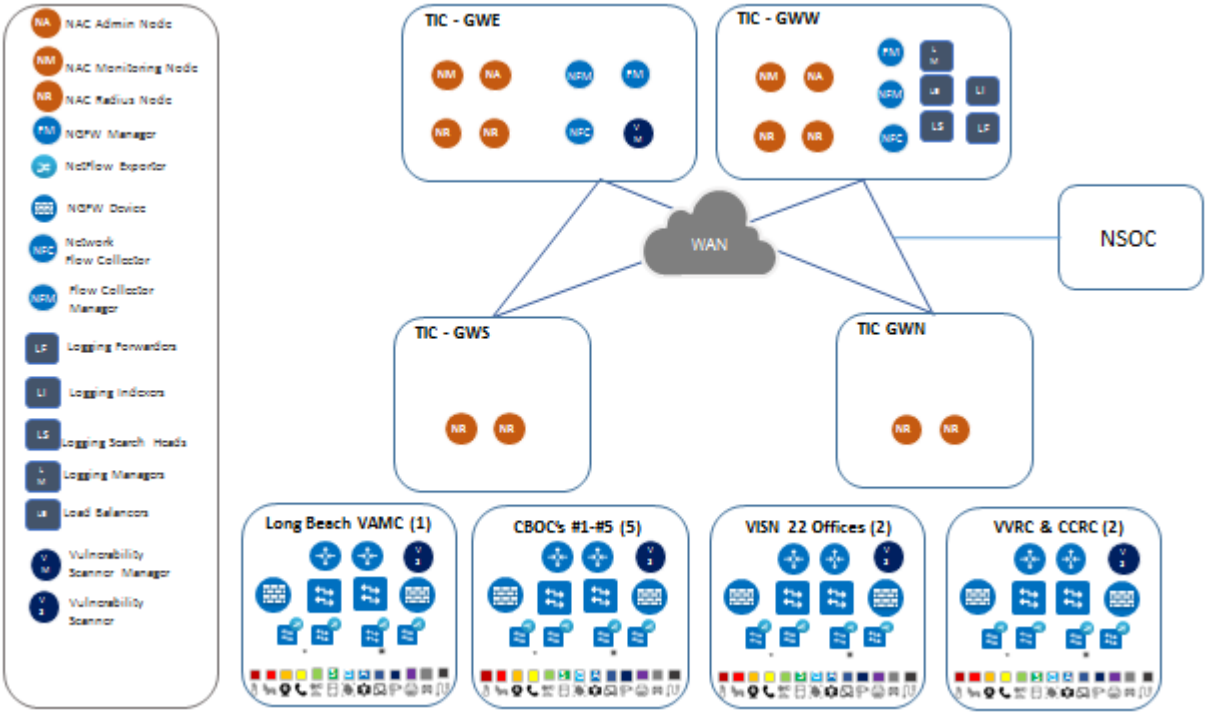
2. Pilot Scope/Scenarios

The Pilot will be the outcome of an IT technical "Integrator" using a suite of technology commercial off-the-shelf (COTS) technologies recognized by industry as leading-edge solutions for cyber security goals and data isolation, information availability, assurances

down to device of status, an alerting functionality, heuristics, traffic analysis, and the prevention of data exfiltration (data leakage) from VA.

3. High Level Pilot Architecture –

Below is a high level representation of VA's existing networking architecture. Medical Devices and Special Purpose Systems are connected at the local facility level through wired or wireless connections to switches and routers that in turn connect to the VA's Wide Area Network (WAN).



Solution management components shall be installed in each of the four primary VA Trusted Internet Connection (TIC) gateways, the NSOC, and the pilot boundary area.

3.1.1. Pilot Location

The selection of the proposed pilot location was determined from a list of sites recently upgraded networking and switching components. A site survey shall be accomplished in order to determine the exact Bill of Materials (BOM) is required both in terms of hardware and software for the pilot solution. It is known that the MedFusion pilot will consist of the Long Beach VA Medical Center (VAMC) itself, all five (5) outlying Community-Based Outpatient Clinics (CBOC), VISN 22 offices (networking Office and Contracting Office), the Veteran Vocation Rehabilitation Center (VVRC), and the Capitol Regional Readiness Center (CRRC). There are no-known additional external partner connections (at this time), connections to the TIC's and the command center at the NSOC.

4. Success Criteria

The following draft criteria reflect the capabilities, data and metrics desired at the different points of the MedFusion pilot architecture to support the analysis and recommendations for the MedFusion pilot effort.

4.1. IT Management/Data Center

A. The solution shall provide highly available management with all networked medical devices and special purpose systems and components capable of supporting the pilot location, it's CBOC', the TICs and bi-directional communication to/from the NSOC.
B. The solution shall provide aggregated dashboards and alerting for all components.
C. The solution shall meet VA Office of Information and Technology (OI&T) standards for device hardening. VA's Continuous Readiness in Information Security Program baselines are used to standardize the configurations of servers/appliances. Standards are located on internal VA URL: https://vaww.sde.portal.va.gov/svcs/sma/BCM/SitePages/Home.aspx
D. The solution shall meet VA OI&T standards for management authentication.
E. The solution shall provide detailed alerting: Not only a customizable dashboard alert but the capability to notify via personnel via mobile telephone and email/text as well.
F. The solution shall describe a consolidated workflow (i.e., a Use Case) for medical device and special purpose system onboarding, containment and isolation.
G. The solution shall differentiate access for different VA administrative roles: customizable and downloadable Role-Based Access Control (dACL's, etc.)
H. The solution shall provide differentiated authentication, and authorization policies based on the medical device or special purpose system type and impact on mission risk.
I. The solution shall aggregate event and alert information from all system components then analyze the data to identify threats to the biomedical device network. In addition, VA personnel from various disciplines will offer perspectives and insight into configuration processes, and changing scenarios for the test site and observations observed from the NSOC, TIC, and other disciples which are stakeholders in this MedFusion pilot. The team expects flexibility to change pilot parameters based on changes to best practices and allow for expansion of observations and viewpoints regarding how the solution is being tested. Remote access to authorized SME's to view, manipulate, and use configurable dashboards. This includes access to viewing of all equipment configurations of equipment and understanding as data is traversing the VA Enterprise Intranet as this allows for greater insight and facilitates more suggestions and learned insight.

4.2. MedFusion Pilot Hospital

A. The solution shall provide a phased unobtrusive approach to implementing security controls with no mission impact measured in medical device availability.
B. The solution shall isolate medical devices and special purpose systems on the same Virtual Local Area Network (VLAN) using at least two types of security controls.
C. The solution shall profile medical device communications and behavior. - There are downloadable medical device profiles in a database that can categorize behavior and communications. (These should be available from the manufacturers and resellers.)
D. The solution shall be able to identify and contain complex threats. For example, With Healthcare security at the height of media coverage, it's important to prepare for Zero Day complex threats that can target medical devices and IoT/SPS within the VA sites. In addition, the solution shall be ready to properly handle a cyberattack from multiple directions at once (e.g. Botnet)
E. The solution shall restrict unknown medical devices with minimal mission impact. - Unknown medical devices should be put into quarantine until approved by BME/OIT staff/site personnel
F. The solution shall automatically identify all MD/SPS end-point devices and the type and communication characteristics of the item.
G. The solution shall identify when devices are added and when devices are removed from the network, and, in addition, characterize and identify normal and abnormal heuristics of the end-point devices.
H. The solution shall identify medical device or special purpose system communications that do not comply with the security profile of the system. Automated reactionary action is required rather than relying on Admin intervention (e.g. quarantining compromised devices).
I. The system shall identify vulnerabilities on medical devices and special purpose systems without agents or credentialed scans.

4.3. Community Based Outreach Clinic

A. The solution shall provide a phased approach to implementing security controls with no mission impact measured in medical device availability.
B. The solution shall isolate medical devices and special purpose systems on the same VLAN using at least two types of security controls.
C. The solution shall profile medical device communications and behavior.
D. The solution shall be able to identify and contain complex threats.
E. The solution shall restrict unknown medical devices with minimal mission impact.
F. The solution shall automatically identify the medical device or special purpose system type and communication characteristics.
G. The solution shall identify medical device or special purpose system communications that do not comply with the security profile of the system.

H. The system shall identify vulnerabilities on medical devices and special purpose systems without agents or credentialed scans.

5. Additional Assumptions or Constraints

Dashboard: Shall have a customizable administrative and network dashboards with real-time data updates, which over time, will aid in facilitation/reduction/elimination the need ACLs, reducing the TCAM usage on the switches, and contain a mobile platform for administrators to monitor activity remotely, have effective MDIA in place, have an emergency plan with respective Points of Contact in a Centralized solution (not region by region/district by district)

HW/Software: Shall be upgradeable and patch-able without delays in 510K FDA certification clauses, and IAW CRISP baseline configuration guidelines

Visual Interfaces: Dashboard presentation and analytics shall be relatively easy to navigate, scalable (from macro to micro granularity), and Section 508 compatible

Security: Shall protect the medical devices and IoT devices within the pilot boundary at the selected pilot site to prevent an attacker from entering and pivoting within the network – all while ensuring that as the network surface area expands and/or contracts that full functionality of performance remains. Also shall be easily monitored and prevent/stop attacks in progress and eliminate viruses.

Pilot Working Group: The VA will have continuous input from an engineering and business perspective for pilot use including al processes including report generation and be involved in the tuning of the configuration process. The pilot expects an outcome whereby Lessons Learned will be aided through interaction with the pilot vendor to allow for an expansion of through observations and suggested viewpoints for the goal of regarding the solution that is being tested, and learning the strengths and weaknesses of the pilot to facilitate a recommendation for further consideration additional capabilities and security of VA end-point devices. Remote access for use of the dashboards is required, as well as, access to all hardware and software as-built drawings.