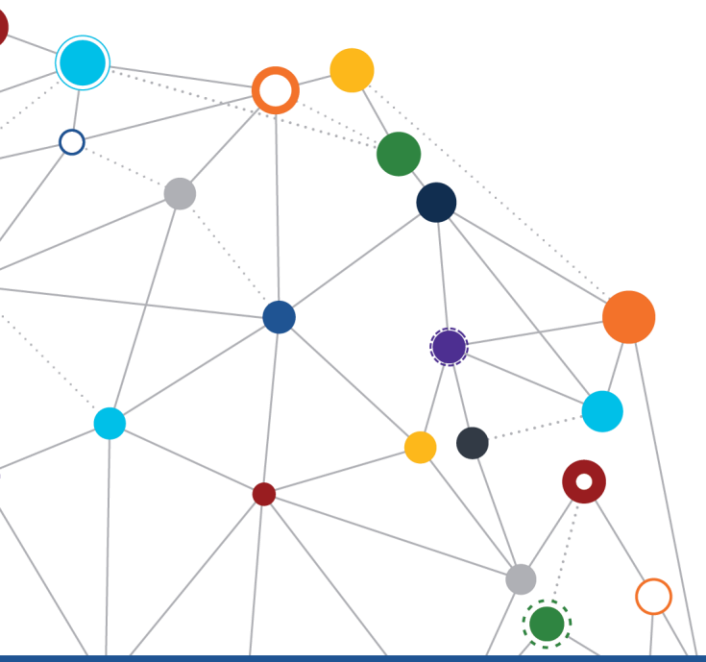
OFFICE OF
INFORMATION
AND TECHNOLOGY

3D Printing Enterprise Design Pattern

Network Design and Security

July 2019 | Enterprise Program Management Office



VA | U.S. Department of Veterans Affairs
Office of Information and Technology

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	2/2019	3D Printing Segment 1: Network Design and Security
2.0	6/2019	Updated to include description of interim and future state capabilities; adjudication of stakeholder comments.

1 Context

Three-dimensional (3D) printing is utilized at a small number of facilities at the Department of Veterans Affairs (VA). Significant developments have ensued over the past few years as the VA Center for Innovation (VACI)[1] continues to partner directly with 3D printing hardware (HW) and software (SW) manufacturers. As a result, 3D printed objects are currently being used to help Veterans within a wide range of use cases. As this technology continues to mature, more 3D printers are expected to be utilized at VA facilities.

The primary audience for this Enterprise Design Pattern (EDP) segment includes information technology (IT) system architects, network security administrators, 3D printing network administrators, and hospital administrators at VA hospitals who are interested in adding a new 3D printer or who utilize an existing 3D printer.

2 Problem

Currently, there are a limited number of standalone 3D printers at VA hospitals. The 3D Printing Committee has identified a need to increase utilization and access to these printers. Figure 1 illustrates three key pillars for establishing an agile architecture that can advance the current 3D printing technology landscape at VA, supporting future growth as the number of 3D printers increase in quantity at VA hospitals and facilities. Each pillar is addressed in a separate *3D Printing* EDP segment document. This EDP document focuses on the area that is highlighted in red.[2]

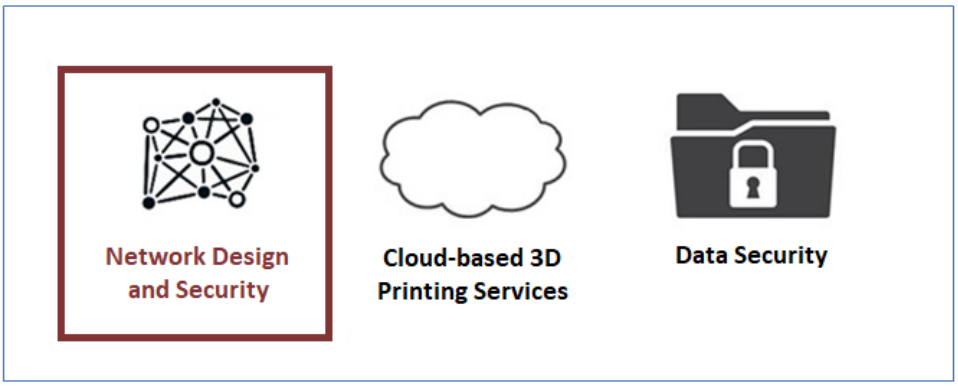


Figure 1: VA 3D Printing Segment Topics[3]

[1] Refer to the VA Center for Innovation (VACI) at https://www.innovation.va.gov/.
[2] Refer to the *3D Printing* EDPs at https://www.oit.va.gov/library/recurring/edp/index.cfm.
[3] Source: Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) EDP Team from information obtained from VA Subject Matter Experts (SMEs).

3 Approach

This section addresses solutions for the interim and future state of 3D printing at VA.

3.1 Network Design and Security

3.1.1 Network Topology

Capability for the Interim and Future State

The network design is influenced by the security classification level for each 3D printer and 3D printing SW. In conjunction with network security administrators, VA hospital administrators adding a new printer, or maintaining an existing 3D printer, **must** conduct the following steps to determine the security classification level and network design:

- Utilize VA Directive 6550 to determine whether a device or system qualifies as a medical device/system.[4]
- Determine if the printer is classified as a medical device by evaluating it against the criteria stipulated in Appendix B of VA Directive 6550.[5]
  - Medical devices/systems must reside in a Medical Device Isolation Architecture (MDIA) Virtual Local Area Network (VLAN).[6]
- If the 3D printer is not deemed a medical device/system, classify the 3D printer as an Internet of Things (IoT)/Special Purpose System (SPS) device and follow IoT VLAN requirements.[7]
- If the 3D printer is determined to be a stand-alone device, and is not connected to a network, classify the 3D printer as a Special Devices Isolation and Architecture (SDIA).

The diagram in Figure 2 depicts the VA interim state high level architecture of 3D printing systems.

---

[4] Refer to VA Directive 6550, *Pre-Procurement Assessment for Medical Device/Systems*, February 20, 2015, at https://www.va.gov/vapubs/search_action.cfm?dType=1.

[5] Refer to the VA Directive 6550, *Pre-Procurement Assessment for Medical Device/Systems*, February 20, 2015, page B-1 to B-2, at https://www.va.gov/vapubs/search_action.cfm?dType=1.

[6] A MDIA is a dedicated VLAN, configured with an access control list (ACL). The MDIA ACL is used to strictly limit external access of the endpoint devices to other devices, systems, and IT resources. For more information on MDIA ACLs, refer to *Volume II, Medical Programs and Information Technology Programs, Congressional Submission, FY 2019 Funding and FY 2020 Advance Appropriations*, on page IT 564 at https://www.va.gov/budget/docs/summary/fy2019vabudgetvolumeiimedicalprogramsandinformationtechnology.pdf.

[7] Refer to the *Internet of Things (IoT)* EDP at https://www.oit.va.gov/library/recurring/edp/index.cfm.

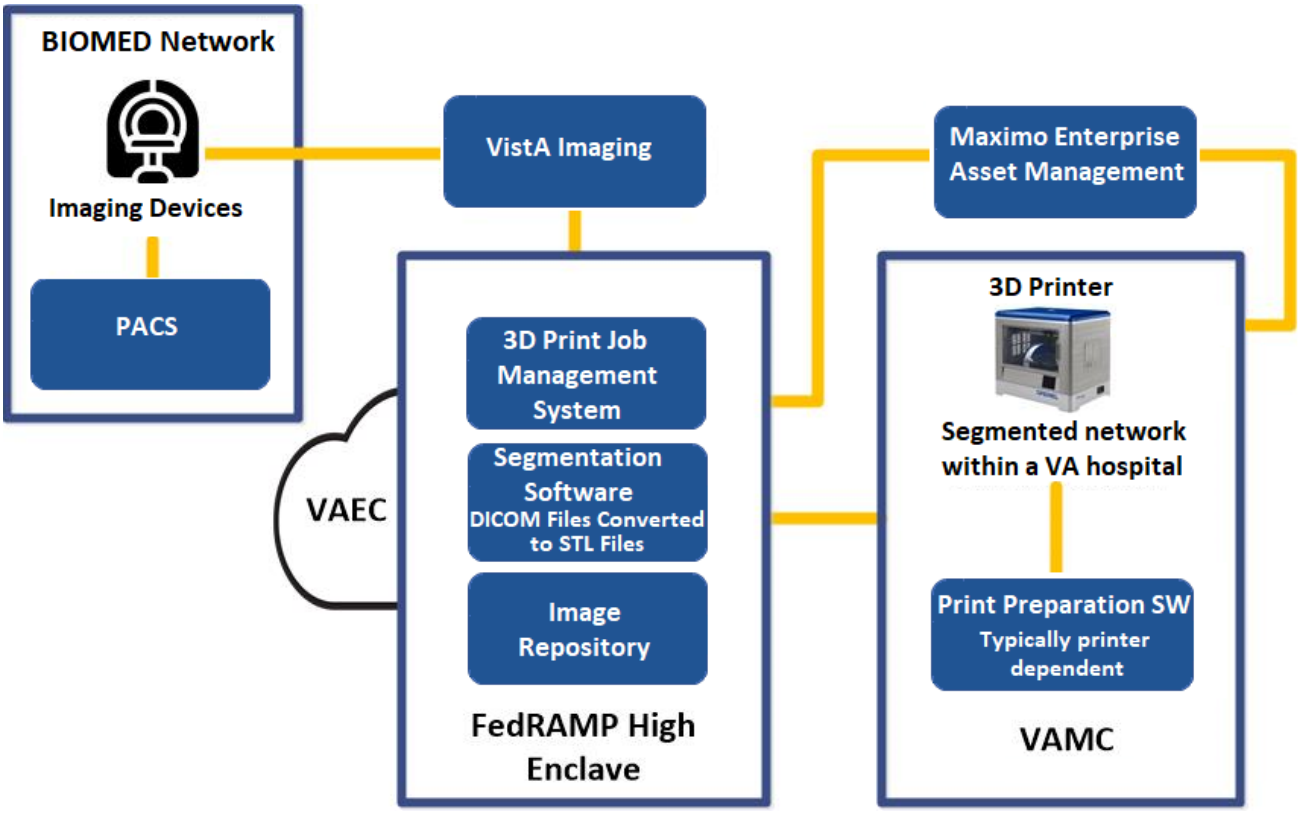


Figure 2: Interim State VA 3D Printing Architecture[8]

[8] Source: Figure 2 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) EDP Team from information obtained from VA Subject Matter Experts (SMEs). The VistA Imaging Overview can be referenced at https://www.va.gov/health/imaging/overview.asp.

3.1.2 Asset/Configuration Management

Capability for the Interim and Future State

As more hospitals and other VA facilities seek to acquire 3D printers, it will be important for VA to manage 3D printers at an enterprise level. This ensures that new 3D printers introduced to the VA network are properly secured and maintained, meeting an appropriate level of quality control. The hospital administrators who are responsible for adding an existing 3D printer **must** incorporate the following actions:

- Register the 3D printer with the Maximo Enterprise Asset Management System. The Service Oriented Architecture Research and Development (SOARD) Project administers VA's enterprise-wide asset management system.[9]
- Report to SOARD prior to procurement.
- Follow a common baseline configuration (e.g., security patches, firmware updates, etc.) that is established by ITOPS to ensure common configuration control.[10]
- Acquire approval for all software/firmware updates through the Configuration Management (CM) Process.
- Use a site-to-site VPN connection with a Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA)[11] for vendor access to internal VA systems (for any purpose; e.g., software/firmware updates).

In addition, hospital administrators who are responsible for adding an existing 3D printer should consider incorporating the following actions:

- Automate software/firmware updates after CM approval.
- Ensure that 3D printing network administrators configure dashboards at the hospital, within the Veterans Integrated Service Network (VISN), and/or at the enterprise level. Dashboard information will be utilized by the Print Job Management System for print job routing. Dashboards deliver insight and identify areas of improvement by tracking the print job activity; and by displaying other key

[9] Refer to VHA SOARD Project at https://vaww.va.gov/plo/soard/about/index.asp.
[10] Refer to the Department of Veterans Affairs OIT Printer and Multifunction Devices Baseline Configuration at https://vaww.vashare.oit.va.gov/sites/ois/KnowledgeService/SecurityDocuments/Multifunctional%20Devices/Printer%20Multifunction%20Devices%20Baseline%20Configuration.pdf. Refer to the National Institute of Standards and Technology (NIST) *Special Publication 800-53* for establishing a baseline configuration (CM-2) at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[11] Reference MOU ISO Templates at https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/ESO%20Library/Forms/AllItems.aspx?RootFolder=%2Fsites%2Finfosecurity%2Ffieldsecurity%2FESO%20Library%2FMOU%20ISA%20Templates&FolderCTID=0x0120002326DA99653E964BAD0FD5F39F245C85&View={5EE98236-FE0A-4AC7-9FE1-6AF9B686AB0D}

performance indicators that monitor the health of 3D printers. The 3D Printing Advisory Committee is still reviewing the required contents for the dashboard.

3.1.3 User Level Security

Capability for the Interim and Future State

3D printing network administrators and network security administrators **must** ensure user level security by implementing the following actions:

- Establish a 3D printing user group with Role Based Access Control (RBAC) using the VA enterprise directory.
- Establish user group management at the enterprise level. An administrator at the enterprise level must have the ability to add/remove users at the local level.[12]
- Regulate access control to 3D printers and 3D printing SW with RBAC, through Identity and Access Management (IAM).[13]

Compliance with these standards apply to the following scenarios:

- Bringing existing 3D printers onto the VA network
- Bringing new 3D printers onto the VA network

4 Impacts

If project teams do not adhere to 3D printing network design and security guidelines, the following negative impacts may be realized:

- 3D printers are more vulnerable to internal and external cyber attacks.
- With no central management, there is greater difficulty in ensuring that 3D printers are utilizing the security/firmware updates.
- There is inefficient use of existing 3D printing resources.

[12] Refer to NIST 800-53 as a reference for account management considerations (AC-2) at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
[13] Refer to the *Identity and Access Management (IAM) Authorization Planning* EDP at https://vaww.ea.oit.va.gov/enterprise-design-patterns-reports/.

Appendix A: References

- NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- VA Directive 6550:
- https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=790&FType=2
- VA Directive 6551: https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=829&FType=2
- VA EDPs: https://www.oit.va.gov/library/recurring/edp/
- VA DEA User Stories: https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/External%20Documents/DEA%20User%20Stories%20v2.3%20(ACTIVE).doc
- VA TRM: http://trm.oit.va.gov/ and https://www.oit.va.gov/services/trm/
- VIP Guide: https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371

Appendix B: Description of Complex Figures

Figure 1: The VA 3D Printing Pillars graphic shows three pillar images of agile architecture for 3D printing at VA. The first is titled Network Design and Security, with an image of interconnected lines and points surrounded by a red border to denote that it is the subject of this segment. The second image is titled Cloud-based 3D Printing Services, with an outline of a cloud. The third image is titled Data Security, with an image of a lock on a file folder.

Figure 2: The Interim State VA 3D Printing Architecture image displays a work flow that incorporates three text boxes: the BIOMED Network text box, the FedRAMP High Enclave text box, and the VAMC text box. The image uses a solid line to illustrate the flow from the PACS label to the Imaging Devices icon in the BIOMED Network text box, to the VistA Imaging label adjacent to it. The VistA Imaging label connects to the VAEC icon, which is overlapped by the FedRAMP High Enclave text box to show that the FedRAMP High Enclave is part of the VAEC. The FedRAMP High Enclave text box vertically displays a 3D Print Job Management System label, a Segmentation Software with DICOM Files Converted to STL Files label, and to an Image Repository label. The FedRAMP High Enclave text box leads externally to the Maximo Enterprise Asset Management label, which leads to the VAMC text box. The VAMC text box displays the 3D Printer icon, which leads to the Segmented Network within a VA Hospital text box, and then leads to the Print Preparation SW label, that is noted as typically printer dependent.