VistA Data Project Security Recommendations Addendum

Sponsor: Department of Veterans Affairs
Contract No.: VA118-15-D-0004
Task Order: VA118-15-J-0136

January 18, 2017

McLean, VA

MITRE

Revision History

Version	Date	Brief Description of Revision	Change Entered by
1.0	18 January 2017	Final Recommendations	MITRE

Table of Contents

1. Introduction 1
2. Security Requirements and the SDLC 1
3. Authentication 2
4. Authorization and Access Control 2
5. Data Protection 3
6. Audit 4
7. Reference/Bibliography 5

1. Introduction

This document is an addendum to "VistA Data Project Integration Recommendations" release 29 April, 2016 [1]. Refer to the main document for additional recommendations.

As only a pilot demonstration, VistA Data Project (VDP) has not yet addressed security capabilities needed for an ATO. For a summary of the VDP's initial pilot demonstration scope, refer to "VistA Data Project Prototype One Pager". [2] As the project moves from the pilot stage to the development and deployment of an operational capability, VDP (and other supporting projects) must address aspects of authentication, authorization and access control, data protection, audit, and SDLC security requirements. Accordingly, recommendations in this addendum frequently cover follow-on activities and may involve outreach to other VA development groups, projects, or organizations providing enterprise security capabilities. These recommendations are intended to assist with the development of an operational capability that is secure and compliant with Federal statutes and regulations, in addition to VA security policies.

Each of these areas is addressed in the sub-sections that follow in rough order of the urgency attached to the particular concern. The order also represents dependencies between security topics in that areas to addressed later in the VDP capability development lifecycle have dependencies on areas that should be addressed earlier.

2. Security Requirements and the SDLC

As VA moves to the Veteran-focused Integration Process (VIP), their lean agile framework for systems development, the need to identify security requirements early becomes even more urgent than it was when VA used a waterfall development model. Many security requirements transcend the normal sprint cycle and short development timelines, in that they represent foundational capabilities that must be in place early in order to support secure deployment, assessment, or validation for other security requirements.

Security requirements should be categorized as to whether they are purely functional in nature, compliance-related, or both. Examples of the former include Attribute-based access control (ABAC), a capability that is a stated VA goal and that aligns with VA's Enterprise Security Architecture, but that is not required by regulations, statutes, or VA policy. [2] [3] An example of a purely compliance requirement is the mandated use of Identity and Access Management authentication services. [4] The specific manner of authentication service integration is not specified, merely the compliance aspect. An example of requirement that is both compliance-related and functional is the need to support PIV-only Authentication (POA). [5] This requirement, is one that should be addressed early in the systems development phase because it is foundational, supporting other capabilities such as access control and audit.

Identification and categorization of security requirements, the "racking and stacking" of capabilities, begins with risk analysis and the application of the NIST Risk Management Framework (RMF). [6] Analysis of vulnerabilities and threats, identification of risks, categorization of supporting systems as to their security impact level, identification and tailoring of security baselines, and selection of security controls all inform the process of identifying security requirements and provide insight into the choice of particular security capabilities. Once chosen, security capabilities can be assigned to functional or compliance Epics and prioritized for purposes of backlog assignment. Foundational capabilities, in other words those capabilities that must be in place to support secure deployment across many sprints, should be given the highest priority.

Table 1. Recommendation – Early Risk Analysis

Observation	Executor	Recommendation
Agile development, with many user-facing deployments, necessitates early identification and categorization of security requirements, along with assignment to appropriate Epics.	VDP	Engage in early risk analysis and application of the NIST RMF in order to 1) Satisfy the requirements of Handbook 6500, and 2) Identify appropriate security capabilities for VDP that can then be categorized and prioritized for efficient and secure implementation.

3. Authentication

VDP's Local VistA Data Model (VDM) and Master VDM (MVDM) layers handle Sensitive Personal Information (SPI), so the systems that support VDP will likely be categorized (per FIPS 199) as having a high security impact for confidentiality. [7] Accordingly, VDP must be compatible with authentication mechanisms of sufficient strength to be able to assure the identity of a user with high confidence. VA mandates the use of cryptographically 'strong', 2-factor mechanisms such as PIV cards for such applications. [5]

In addition, VDP intends to provide access control as a capability available to the MVDM layer. This layer, referred to as the *Security Model*, provides ABAC that will leverage security-relevant VistA data attributes. [8] Authentication data contains the security relevant attributes of the user and must be available and in a form that can be consumed by components that calculate and enforce authorization decisions. This presents an additional challenge for VDP since OI&T Identity and Access Management (IAM) services currently only support Security Assertion Markup Language (SAML) based authentication assertions. Consequently, VDP must have a method for processing authentication assertions for a particular user in order to enable access control.

VDP's object model is based on JavaScript Object Notation (JSON)-LD. So it may be necessary to provide functionality to bridge between JavaScript and Simple Object Access Protocol (SOAP) for the security context provided by IAM services such as Single Sign-on External (SSOe) and Single Sign-on Internal (SSOi). This may take the form of a converter that can translate between SAML and JSON Web Tokens (JWT) and could be implemented by VDP developers. However, a preferable approach, since VDP is a project that requires a JSON-based solution for authentication contexts, would be to engage with other projects to determine the requirements of the solution, and then to engage IAM for development and deployment. The VDP project could, in absence of IAM resources, serve as the initial capability demonstrator for the solution once the requirements have been agreed upon.

Table 2. Recommendation – SAML / JSON Authentication Support

Observation	Executor	Recommendations
VDP, as well as a number of other VistA data access solutions, have a need for JSON-based representation for 'strong' authentication assertions. These are not currently supported by IAM which only supports SOAP-based, SAML assertions.	VDP and other VA projects using JSON-based data models	Cooperatively determine the exact requirements for JSON-based, strong, authentication assertions, using JWT or other applicable standards.
	VDP	Engage with OI&T IAM to request new JSON-based authentication support.
	OI&T / IAM	Implement JSON-based authentication assertions and, optionally, SAML/JWT translation capability as a VA enterprise authentication service. Integrate with SSOi and SSOe.

4. Authorization and Access Control

The VDP designers have identified fine-grained, attribute-based access control as an important security requirement. [8] The intent is to provide access control as a capability that can be invoked by the MVDM layer with security relevant metadata added directly to the resources. Consequently, addressing the lifecycle of security attributes from identification, through provisioning and population, to replacement or retirement, will be a challenge for VDP as it moves out of the pilot stage. In addition, VDP will also have to deal with the identification, representation, and maintenance of access control policies. VDP should engage as soon as is practical with VA's data governance bodies in order to determine the alignment and the expected security-relevant attributes with other VA projects and organizations that have similar questions. The ASD Security Architecture Working Group (SAWG) and Data Governance Council are good starting points.

Table 3. Recommendation – Attribute Lifecycle

Observation	Executor	Recommendations
VDP will have to undertake the challenge of providing some level of support for managing the lifecycle of security-relevant attributes and access control policies.	VDP	Identify VDP requirements for security attribute support on VistA data objects and authenticated users. Identify illustrative VistA access control policies that can be used as examples for identification of policy support requirements. Identify and document the policy requirements.
		Engage with VA data governance bodies such as the ASD SAWG and Data Governance Board to ensure that efforts to define and manage security-relevant attributes and policies are not duplicated and that VDP requirements are included in similar discussions by bodies focused on enterprise security and capability planning.
	OI&T / EPMO and OI&T / ASD	Establish lifecycle policies and procedures for attribute and access control policy management, provisioning, maintenance, and retirement/replacement.

In order to provide the greatest level of agility with respect to developing its access control solutions, VDP's development teams should not try to invent their own solutions for managing the attribute or policy lifecycles, encoding and managing access control policies, or providing authorization and access control services. Rather, VDP should leverage the existing fine-grained access control capability provided by IAM's Specialized Access Control (SAC) capability. This will allow VDP to offload this security capability to an existing enterprise-class solution and to adapt as VDP development teams prototype new or refined policies and attribute schemes. Moreover, as VA moves toward resolving issues related to providing fine-grained access control across the enterprise, VDP will be in a position to take advantage of those changes where they are likely to be deployed first…in IAM SAC.

Table 4. Recommendation – Leverage IAM Specialized Access Control

Observation	Executor	Recommendations
Implementing and managing all of the elements required by a fine-grained, ABAC or other, access control solution is difficult enough even when all of the requirements for attributes and policies are known in advance. (Not the case currently for VDP or VA more generally.)	VDP	Engage with OI&T / IAM to assess the suitability of IAM SAC for supporting ABAC in VDP.
	VDP and OI&T IAM	Assuming IAM SAC proves suitable for supporting VDP's ABAC requirements, integrate IAM SAC for providing fine-grained access control support.

5. Data Protection

As mentioned previously, the security impact level of systems supporting VDP is likely to be high due to the presence of Personal Health Information (PHI) and Personally Identifiable Information (PII). [7] [9] Such systems must preserve the confidentiality of data-at-rest (DaR), and typically employ encryption to do so.

VDP's Security Model proposes to support fine-grained access control by adding security-relevant metadata (for resources) directly to the primary data model. Consequently, an end-to-end encryption system, where the data content is opaque to the VDP solution and largely ignored, would not be sufficient. Security-relevant data attributes must be available 'in the clear' at least as long as they are being used in producing authorization decisions in VDP's Security Model layer. That being the case, a system-level (filesystem based, for example) encryption solution is preferable to resource-level encryption provided by FileMan, another DBMS, or another application layer.

Table 5. Recommendation – Data at Rest Encryption

Observation	Executor	Recommendation
VDP must preserve the confidentiality of DaR while also making security-relevant metadata available to components that support calculation and enforcement of authorization decisions.	VDP	Identify a suitable base-level (file-system or other similar) solution in order to meet confidentiality requirements, transparently, and with minimum impact to VDP's Local VDM and MVDM layers.

6. Audit

Robust and effective audit capabilities serve many purposes in an enterprise from enhancing situational awareness to threat detection and mitigation. As with many VA projects that externalize VistA data, VDP has not yet decided on the requirements of their audit capability. So attempting to make recommendations in this area may be premature. However, as VDP moves out of the pilot stage, the following security-related questions should be addressed as part of audit requirements definition:

- **Should/will the audit capability be integrated with Continuous Diagnostics and Mitigation (CDM)?**

  VA is currently moving from an implementation of DHS CDM Phase 1—which is concerned with hardware and software inventories, vulnerabilities, and configuration—to CDM Phase 2 which is concerned with least privilege and infrastructure integrity. VDP's audit capability, indeed the audit capabilities of any solution that provides access to VistA data, could be leveraged to provide information on security-related behaviors, credentials usage, authentication, and access control, all of which are used in CDM Phase 2. Decisions on what events to audit, how often, how to normalize audit data, and how to make data available to VA CDM or VA Security Information and Event Management (SIEM) tools will inform the requirements for audit.

- **Should VDP leverage an enterprise audit capability, or should VDP work with other VA projects to define common audit standards?**

  Ideally, an enterprise audit solution, one that satisfies CDM requirements and integrates with existing CDM and SIEM tools, would be available to VDP developers, but in absence of such a solution, VDP could work with other VistA programs and with the FileMan program to define the standards for audit capabilities, audit granularity, and audit data. These capabilities could be prototyped by VDP as a demonstration capability and proposed as an internal VA standard for healthcare systems.

7. Reference/Bibliography

[1] The MITRE Corporation, "VistA Data Project Integration Recommendations," 2016.

[2] The MITRE Corporation, "VistA Data Project Prototype One Pager," 2016.

[3] VA Office of the Assistant Secretary for Information and Technology, "ECST Domain Report: Access Control, Identification, and Authentication," U.S. Department of Veterans Affairs, Washington, DC, 2015.

[4] VA Office of Information and Technology, "VA Enterprise Design Patterns: Privacy and Security Enterprise Authorization, Version 1.0," U.S. Department of Veterans Affairs, Washington, DC, 2016.

[5] VA Office of Information and Technology, "VA Enterprise Design Patterns: Privacy and Security and User Identity Authentication, Version 2.0," U.S. Department of Veterans Affairs, Washington, DC, 2016.

[6] VA Office of the Deputy Assistant Secretary for Information Security, *Memorandum: Mandatory Use of PIV Multifactor Authentication to VA Information System - VAIQ 7613595,* Washington DC: U.S. Department of Veterans Affairs, 2015.

[7] VA Office of the Assistant Secretary for Information and Technology, "Handbook 6500: Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program," U.S. Department of Veterans Affairs, Washington, DC, 2015.

[8] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems," U.S. Department of Commerce, Washington, DC, 2004.

[9] Veterans Health Administration, "VISTA Data Project," US Departmenty of Veterans Affairs, 2016.

[10] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 200: Minimum Security Requirements for Federal Information and Information Systems," U.S. Department of Commerce, Washington, DC, 2006.