



**Exhibit 4.7  
Software Assets  
Effective June 11, 2021**

**VA-210517-NTT - Messaging Services**

**COMMONWEALTH OF VIRGINIA  
VIRGINIA IT AGENCY (VITA)  
SUPPLIER STRATEGY AND PERFORMANCE DIVISION**

**11751 MEADOWVILLE LANE  
CHESTER, VIRGINIA 23836**

## Software Assets - Enterprise (Messaging Services)

Notes:

Note 1: License count for a ██████████ Products is estimated to be 130 and includes licenses for ██████████

Note 2: Counts for SQL 2000 and 2005 should be under 10 (not supported by MS any longer)

Note 3: Counts for SQL 2008 2012 2014 20 6 are currently only available as a total amount (384)

Note 4: VITA will retain ownership of Microsoft Licenses (for more information on license counts for Windows Server see Exhibit 4.6)

Note 5: VITA will retain ownership of Oracle Database Product Licensing. Estimated License count for Oracle Database is 174 and includes licenses for Oracle Database 10 11 and 12

Note 6: Netbackup Product is estimated to have 6 master licenses (the number listed as the license count for this product). Licensing may also be required for a 1 the nodes in the environment which should be roughly equal to the number of servers in CESC - this number is included in current environment documents. Additionally, netbackup appliances may exist in environment and are not represented in this exhibit

Note 7: License count for ESX Product includes licenses for both ESX (version 4.x) and ESXi (versions 4.1 5.x and 6.x)

Note 8: No available estimate for license counts for these products at the moment

Virginia Information Technologies Agency

Software Assets (MSI)

Entry Reference Number	Software Type (FROM 2.6)	Supplier System Name	Vendor	Software Product Name	Version (as of Effective Date)	Description	Access to be Provided to Commonwealth (V A Agencies, other suppliers)	Contracting Party	License Owner
MSI - 4.6 - 30	Data Warehouse System: Project Portfolio Management and Project Management Reporting System: Document Data Store Security Clearance System: Risk Management System: Security Configuration Management System: Content Management System	CENTER Suite	Microsoft	Microsoft SharePoint Server	Current	Documentation Management component of the CENTER™ suite	Direct access is provided to VITA and Cus other personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 31	Data Warehouse System	CENTER Suite	Microsoft	Microsoft SQL Server Enterprise	Current	Data Warehouse and Reporting component of the CENTER™ suite	Direct access is provided to VITA and Cus other personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 32	Project Portfolio Management and Project Management Reporting System		Microsoft	Microsoft Project Server	Current	Component of the CENTER™ suite provides enhanced integration and reporting on managed project schedules and resources.	Direct access is provided to VITA and Cus other personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 33	Billing, Changeback and Utilization Tracking System		DigitalFuel SV (formerly VMware vRealize Business Enterprise)	Digital Fuel IT Business Management	Current (8.5)	Provides a transparent view and control over the cost and quality of IT services.	Direct access is provided to VITA and Customer personnel consistent with security policy set by VITA. Due to the potential ally sent to maintain the information, SAIC cannot capture VITA and the Commonwealth agencies will be subject to direct access to this system to a subset of individuals within each participating Agency. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 34	Information Security Management System (ISMS)				Current	Performance of vulnerability scanning: support of risk assessment	For information security purposes, SAIC recommends the Commonwealth Agency and Supplier conduct the access to defined subsets of ISMS data via the Keystone Edge components. SAIC does not anticipate recommending direct Commonwealth Supplier access to other components of the ISMS. In all cases, access to SMS data and components will be governed by, and consistent with, VITA information security policy.		
MSI - 4.6 - 35	Information Security Management System (ISMS)				Current	Provides a detailed analysis and visualization of machine data gathered from the weblogs, application logs, sensors, devices, and so on, that comprise your IT infrastructure business.	For information security purposes, SAIC recommends the Commonwealth Agency and Supplier conduct the access to defined subsets of ISMS data via the Keystone Edge components. SAIC does not anticipate recommending direct Commonwealth Supplier access to other components of the ISMS. In all cases, access to SMS data and components will be governed by, and consistent with, VITA information security policy.	SAIC	SAIC
MSI - 4.6 - 36	Information Security Management System (ISMS)		Gigamon	Encase Forensic	Current (8)	Encase Forensic enables digital investigation. Provides deep forensic investigation capabilities to capture evidence and history of incidents.	For information security purposes, SAIC recommends the Commonwealth Agency and Supplier conduct the access to defined subsets of ISMS data via the Keystone Edge components. SAIC does not anticipate recommending direct Commonwealth Supplier access to other components of the ISMS. In all cases, access to SMS data and components will be governed by, and consistent with, VITA information security policy.	SAIC	SAIC
MSI - 4.6 - 37	Information Security Management System (ISMS)				Current	Simulated phishing attack assessment with email templates, teachable moments and full reporting as well as access to the plug-in knowledge assessment with customizable and predefined assessments, automation and full reporting. The software is locally hosted to provide secure and dynamic reporting. The tagged potential phishing email is used by the AI currently available to a network module in the Educator Platform.	For information security purposes, SAIC recommends the Commonwealth Agency and Supplier conduct the access to defined subsets of ISMS data via the Keystone Edge components. SAIC does not anticipate recommending direct Commonwealth Supplier access to other components of the ISMS. In all cases, access to SMS data and components will be governed by, and consistent with, VITA information security policy.	SAIC	SAIC
MSI - 4.6 - 38	Security Clearance System: Identity and Access Management System				Current	Identity management solution that provides streamlined provisioning, administration, and robust use of user accounts. Vitals includes who is doing what, what kinds of risks that represent, and allows you to take action. It links people, applications, data and devices to create a identity-enabled enterprise.	For information security purposes, SAIC recommends Commonwealth Agencies and Suppliers access IAM for account administration (e.g. provisioning of accounts) via the Keystone Edge suite. SAIC will provide authorized VITA and Commonwealth Agency personnel with direct access to IAM components for audit functions. SAIC does not anticipate recommending direct Commonwealth Supplier access to the IAM solution. In all cases, access to IAM data and components will be governed by, and consistent with, VITA information security policy.	SAIC	SAIC
MSI - 4.6 - 39	Identity and Access Management System				Current	Provides privileged account security. Privileged accounts management software used to administer privileged access to organization's IT assets and enable applications.	For information security purposes, SAIC recommends Commonwealth Agencies and Suppliers access IAM for account administration (e.g. provisioning of accounts) via the Keystone Edge suite. SAIC will provide authorized VITA and Commonwealth Agency personnel with direct access to IAM components for audit functions. SAIC does not anticipate recommending direct Commonwealth Supplier access to the IAM solution. In all cases, access to IAM data and components will be governed by, and consistent with, VITA information security policy.	SAIC	SAIC
MSI - 4.6 - 40	Customer Relationship Management		SevcoNow	SevcoNow	Current	Underlying Software as a Service (SaaS) providing automation for IT Service Management, Project Portfolio Management, Security Incident Management and other functions.	Direct access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA. We anticipate that the IT information for the total host content that is aggregated for public review, as well as additional information and functional capability that will require user-level authentication and authorization. Our solution supports both public and access-controlled content and provides Role Based Access Control (RBAC) to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 41	IT Information Portal: Service Catalog and Request Management System: Asset Management System: Service Level Management and Reporting System: Change Management System: Project Portfolio Management and Project Management Reporting System: Incident Management System: Knowledge Database: Event Management and Correlation System: Problem Management and Known Error Database: Software License Management System: Information Security Management System (ISMS): Service Configuration Management System: Capacity Management System: Configuration Management System: Request Management System: Availability Management System: Cloud Brokerage: Supplier Management: Contract Management		SAIC	Keystone Edge™	Current	SAIC processes automation, workflow, and reporting customization enhancements built on SevcoNow Software as a Service (SaaS).	Direct access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA. We anticipate that the IT information for the total host content that is aggregated for public review, as well as additional information and functional capability that will require user-level authentication and authorization. Our solution supports both public and access-controlled content and provides Role Based Access Control (RBAC) to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 42	Cloud Brokerage				Current	Configuration Management: support of cloud brokerage integration.	Direct access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 43	Cloud Brokerage				Current	Operational Monitoring: support of cloud brokerage integration.	Direct access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 43a	Cloud Brokerage				Current		Direct access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 43b	Cloud Brokerage				Current		Direct access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA. Our solution provides Role Based Access Control to enforce application information security policy and access to this system.	SAIC	SAIC
MSI - 4.6 - 44	Risk Management System		RSA	Active	Current	Enhanced risk management	Access to this system will be limited to individuals authorized by VITA information security policy.	VITA	VITA
MSI - 4.6 - 45	Service Desk Telephony		Genesys Interactive Intelligence		Current		SAIC integration with this component supports management of call data (e.g. call volume, call abandonment rate, call duration, average speed of answer, etc.) directly into the Keystone Edge on a near-real-time basis for reporting and analysis. SAIC provides VITA and other Commonwealth agencies with access to this Keystone-hosted reporting and analysis as authorized by VITA information security policy.	SAIC	SAIC
MSI - 4.6 - 46	Remote administration system			Remote Support	Current		Read-only and reporting access is provided to VITA and Customer personnel, as well as ITSP suppliers, consistent with security policy set by VITA.	SAIC	SAIC