Expressing FedRAMP System Inventory in OSCAL

FRX = FedRAMP Extension		GUIDANCE	Valid Values	Mandatory or Optional?	//component/@type (asset-type)	Inventory-Item	Field/Prop	Cardinality	Level	Metapath or Constraint	Notes
All Inventories	UNIQUE ASSET IDENTIFIER (COMPONENT)	Unique Identifier associated with the asset as described on the instructions page of this template and used consistently across all CSO documentation. For OS/Infrastructure and Web Application Software, this is typically an IP address or URL/DNS name as the component is identified by the scans. For a database, it is typically an IP address, URL, or database name. For containers, it is the repository/image name/version number.	string (unique)		software (image)	Yes	"asset-id" prop	1	Error	context="//(component[@type='software' and ./prop[@name='asset-type' and @value='image']] | inventory-item)" target="." count(./prop[@name='asset-id']) = 1 enforce uniqueness	All inventory items and software images MUST have a Unique Asset ID
	IPv4 Address	If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column. If a device has multiple IP addresses, then include one row in this inventory for each IP address.	ipv4-address	Mandatory for all inventory records.	service ("implementation-point" prop set to "internal"	Yes	"ipv4-address" prop	0+	Warning	context="//(component[@type='service' and ./prop[@name='implementation-point' and @value='internal']] | inventory-item)" target="." count(./prop[@name=('ipv4-address', 'ipv6-address', 'fqdn', 'uri')]) >= 1	All inventory items and internal "service" components SHOULD be reachable via a ntwork, which requires either an IPv4 address, IPv6 address, fully qualified domain name (FQDN) or uniform resource identifier (URI). At least one of these four properties SHOULD be present. More than one in any combination is acceptable. For example, a single asset may have an IPv4 address, IPv6 address, and a FQDN.
	IPv6 Address		ipv6-address		service ("implementation-point" prop set to "internal"	Yes	"ipv6-address" prop	0+			
	DNS Name or URL	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	uri	Optional, unless used as Identifier in vulnerability scans or security assessments.	service ("implementation-point" prop set to "internal"	Yes	"fqdn" prop OR "uri" prop	0+			
	Container Checksum	For containers, each entry should contain the individual checksum of the container in the registry for each of the containers in production that align to that image name/version.	string		software (image)	--	"checksum" FRX	1	Error	context="//component[@type='software' and ./prop[@name='asset-type' and @value='image']]" target="." count(./prop[@name='checksum' and @ns='http://fedramp.gov/ns/oscal']) = 1	Container and operating system *images* MUST have a checksum FedRAMP Extension. Images are always represented as "software" components with an "image" asset type. This is a FedRAMP extension.
	Virtual	Is this asset virtual?	"yes", "no"	Mandatory for OS/Infrastructure. **Containers**, Software, and Database.	as linked	Yes	"virtual" prop	1	Error Allowed Values	context="//inventory-item" target=". | //component[@uuid=./implemented-component/@component-uuid]" count(./prop[@name='virtual']) >= 1 allowed-values (allow-others='no'): 'yes', 'no'	Either the inventory-item itself, or the component linked by the inventory-item MUSThave a "virtual" prop indicating whether the item is a physical device or virtual device, such as a virtual server. Ideally, this should check the inventory item first for this property and only check the linked component if not found at the inventory item. They could legitimately conflict, such as if a physical server inventory-item was instantiated using a virtual "software/image" component.
	Public	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	"yes", "no"	Mandatory for OS/Infrastructure. **Containers**, Software, and Database.	service [implementation-point=internal] or as-linked	Yes	"public" prop	1	Error Allowed Values	context="//(inventory-item | component[@type='service' and ./prop [@name='implementation-point' and @value='internal']])" target="." count(./prop[@name='public']) = 1 allowed-values (allow-others='no'): 'yes', 'no'	All inventory items MUST have the "public" property. All internal "service" components MUST have the "public" property
OS/Infrastructure Inventory	NetBIOS Name	If available, state the NetBIOS name of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	string	Optional, unless used as Identifier in vulnerability scans or security assessments.	No	Yes	"netbios-name" prop	0+	none	//inventory-item/prop[@name='netbios-name']	NetBIOS name is an optional property, but SHOULD be present when the inventory item is assigned a NetBIOS name..
OS/Infrastructure Inventory	MAC Address	If available, state the MAC Address of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	string six two-digit hex values separated by either colons or dashes	Optional, unless used as Identifier in vulnerability scans or security assessments.	No	Yes	"mac-address" prop	0+	none Enforce RegEx	//inventory-item/prop[@name='mac-address'] regex = “^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})|([0-9a-fA-F]{4}\\.[0-9a-fA-F]{4}\\.[0-9a-fA-F]{4})$”;	MAC address is an optional property, but SHOULD be present when the inveontory item has a MAC address. There may be more than one if the inventory item has multiple network interfaces.

FRX = FedRAMP Extension		GUIDANCE	Valid Values	Mandatory or Optional?	//component/@type (asset-type)	Inventory-Item	Field/Prop	Cardinality	Level	Metapath or Constraint	Notes

OS/Infrastructure Inventory	Authenticated Scan	Is the asset is planned for an authenticated scan?	"yes", "no"	Mandatory for OS/Infrastructure, **Containers**. Leave blank for Software and Database.	service [implementation-point=internal]	Yes	"allows-authenticated-scan" prop	1	Error
									Error
									Allowed Values
										context="//inventory-item"
										target=". | //component[@uuid=./implemented-component/@component-uuid]"
										count(./prop[@name='allows-authenticated-scan']) >=1
										--- 	
										context="//component[@type='service' and ./prop[@name='implementation-point' and @value='internal']]"
										target="."
										count(./prop[@name='allows-authenticated-scan']) =1
										--- 	
										context = "///(component | inventory-item)/prop[@name='allows-authenticated-scan']"
										target = "./@value"
										allowed-values (allow-others='no'): 'yes', 'no'
											For each:
											- inventory-item -> component relationship
											- inventory-item without a component relationship; and
											- internal "service" component
											
											there MUST be at least one. at least one "allows-authenticated-scan" property. Ideally, this checks

OS/Infrastructure Inventory	Baseline Configuration Name	Name of the applicable Security Technical Implementation Guide(s) (STIGs), Center for Internet Security (CIS) Level 2 Benchmark (s), or relevant hardening benchmark(s). For STIGs, ensure all relevant STIGs are included:
		- Application Security Requirement Guide (SRG)
		- Network SRG
		- Operating System SRG
		- Policy SRG
			uri	Mandatory for all assets/components	service [implementation-point=internal], software, hardware	Yes	"baseline" link	1+	Error
									Error
										context="//inventory-item"
										target=". | //component[@uuid=./implemented-component/@component-uuid]"
										count(//resource[@uuid=//(component[@type=('software', 'hardware', 'service')] | inventory-item)/link[@rel='baseline']/substring-after(@href, '#')]) >= 1
										----- 	
										context="//component[(@type='service' and ./prop[@name='implementation-point' and @value='internal']) or @type=('hardware', 'software')]"
										target="."
										count(//resource[@uuid=//(component[@type=('software', 'hardware', 'service')] | inventory-item)/link[@rel='baseline']/substring-after(@href, '#')]) >= 1
											For each:
											- inventory-item -> component relationship
											- inventory-item without a component relationship
											- internal "service" component
											- "software" component
											- "hardware" component
											
											there MUST be an "attachment" link that cites a back-matter resource of type "external-guidance" and type class of "stig".

Software and Database Inventories	Software/ Database Vendor	Vendor Name of Container, Software or Database.	string (name of vendor or "Open Source"	Mandatory for Software and Database. Leave blank for OS/Infrastructure.	software	Yes	"vendor-name" FRX	1	Error	context="//inventory-item"
										target=". | //component[@uuid=./implemented-component/@component-uuid]"
										count(./prop[@name='vendor-name' @ns='http://fedramp.gov/ns/oscal']) >= 1
											Every inventory-item MUST have a "vendor-name" FedRAMP Extension either within the inventory-item itself, or within the component linked by the inventory-item

OS/Infrastructure Inventory	Hardware Make	Name of the hardware product	string	Mandatory for OS/Infrastructure, Containers. Leave blank for Software and Database.	hardware	Yes	"vendor-name" FRX				

OS/Infrastructure Inventory	OS Name	Operating System Name and Version running on the asset.	string	Mandatory for OS/Infrastructure, **Containers**. Leave blank for Software and Database.	software (operating-system, container, image)	Yes	"os-name" prop
							OR
							"software-name" prop
								1	Error	context="//inventory-item"
										target=". | //component[@uuid=./implemented-component/@component-uuid]"
										count(./prop[@name=('software-name', 'os-name')]) >= 1
											Every inventory-item MUST have a "software-name" property either within the inventory-item itself, or within the component linked by the inventory-item
											
											We perfer "software-name" in all cases, but will accept "os-name" where appropriate.

Software and Database Inventories	Software/ Database Name	Name of Software or Database product and version number.	string	Mandatory for Software or Database. Leave blank for OS/Infrastructure.	software	Yes	"software-name" prop				

Expressing FedRAMP System Inventory in OSCAL

FRX = FedRAMP Extension		GUIDANCE	Valid Values	Mandatory or Optional?	//component/@type (asset-type)	Inventory-Item	Field/Prop	Cardinality	Level	Metapath or Constraint	Notes
OS/Infrastructure Inventory	OS Version	Operating System Name and Version running on the asset.	string	Mandatory for OS/Infrastructure, **Containers**. Leave blank for Software and Database.	software (operating-system, container, image)	Yes	"os-version" prop OR "software-version" prop	1	Error	context="//inventory-item" target=". | //component[@uuid=./implemented-component/@component-uuid]" count(./prop[@name=('software-version', 'os-version')]) >= 1	Every inventory-item MUST have a "software-version" property either within the inventory-item itself, or within the component linked by the inventory-item We perfer "software-version" in all cases, but will accept "os-version" where appropriate.
Software and Database Inventories	Software/ Database Version	Name of Software or Database product and version number.	string	Mandatory for Software or Database. Leave blank for OS/Infrastructure.	software	Yes	"software-version" prop				

Software and Database Inventories	Patch Level	If applicable.	string	Optional if applicable. Otherwise, leave blank.	software	Yes	"software-patch-level" prop	0 or 1	none	//inventory-item/prop[@name='software-patch-level']
										
										//component/prop[@name='software-patch-level']
											Where applicable the software patch level must be provided; however, there is currently no way to write a constraint that detects whether this information is available for inclusion.
											
											In the future, we could potentially look up the software in a dabase that could tell us.

OS/Infrastructure Inventory	Location	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	string	Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.	hardware	Yes	"physical-location" prop	0 or 1	none	//inventory-item/prop[@name='physical-location']
										
										//component/prop[@name='physical-location']
											Consider expanding to include 'location-uuid' option in addition to cage#, rack#, etc.

OS/Infrastructure Inventory	Asset Type	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)	core OSCAL asset-type allowed values, plus: "image", "container"	Mandatory for OS/Infrastructure, **Containers**. Leave blank for Software and Database.	software, hardware	Yes	"asset-type" prop	1	Error	context="//inventory-item" target=". | //component[@uuid=./implemented-component/@component-uuid]" count(./prop[@name='asset-type']) >= 1	Every inventory-item MUST have an "asset-type" property either within the inventory-item itself, or within the component linked by the inventory-item
OS/Infrastructure Inventory	Hardware Model	Model of the hardware product	string	Mandatory for OS/Infrastructure, ~~Containers~~. Leave blank for Software and Database.	hardware	Yes	"hardware-model" prop	1	Error	context="//inventory-item" target="(. | //component[@uuid=./implemented-component/@component-uuid])/prop [@name='asset-type' @value='hardware']" count(./prop[@name='hardware-model']) >= 1	Inventory-items representing hardware devices, MUST have a "hardware-model" property either within the inveontory-item itself, or within the component linked by the inventory-item. NOTE: Sam Aydlette confirmed that "Containers" is a copy/paste error. This does **not** apply to containers.
OS/Infrastructure Inventory	In Latest Scan	Should the asset appear in the network scans and can it be probed by the scans creating the current POA&M?	"yes", "no"	Mandatory for OS/Infrastructure, **Containers**. Leave blank for Software and Database.	software (image)	Yes	"is-scanned" prop	1	Error	context="//inventory-item" target=". | //component[@uuid=./implemented-component/@component-uuid]" count(./prop[@name='is-scanned']) >=1	Every inventory-item MUST have an "is-scanned" property either within the inventory-item itself, or within the component linked by the inventory-item
Any Inventory	Diagram Label	Label of component as it is found on the boundary diagram in the SSP. It is understood that a single component on a diagram may represent many entries in the inventory	string	Mandatory for all assets/components	software, hardware, service, interconnection	Yes	"diagram-label" (FRX)	1	Error	context="//inventory-item" target=". | //component[@uuid=./implemented-component/@component-uuid]" count(./prop[@name='diagram-label' @ns='http://fedramp.gov/ns/oscal']) >= 1 ----- context="//component[not(@uuid=//inventory-item/implemented-component/@component-uuid) and @type=('hardware', 'software', 'service', 'interconnection')]" target="." count(./prop[@name='diagram-label' @ns='http://fedramp.gov/ns/oscal']) = 1	Every inventory-item MUST have a "diagram-label" FedRAMP Extension either within the inventory-item itself, or within the component linked by the inventory-item. Every hardware, software, service, and interconnection component - not linked to an inventory item - MUST have a "diagram-lable" FedRAMP Extension.
Any Inventory	Comments	Any additional information that could be useful to the reviewer.	markup-multiline	Optional for OS/Infrastructure, Containers, Software and Database.	all	Yes	remarks	0 or 1	none	//(component | inventory-item)/remarks	Comments are optional for both inventory-items and components. No constraint necessary.

FRX = FedRAMP Extension		GUIDANCE	Valid Values	Mandatory or Optional?	//component/@type (asset-type)	Inventory-Item	Field/Prop	Cardinality	Level	Metapath or Constraint	Notes
Any Inventory	Serial #/Asset Tag#	Product serial number or internal asset tag #.	string	Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.	No	Yes	"asset-tag" prop OR "serial-number" prop	0 or 1	none	//inventory-item/prop[@name=('asset-tag', 'serial-number')]	Asset tags are optional. They are appropriate for inventory-items, especially hardware items
Any Inventory	VLAN/ Network ID	Virtual LAN or Network ID.	string	Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.	No	Yes	"vlan-id" prop OR "network-id" prop	0 or 1	none	//inventory-item/prop[@name=('vlan-id', 'network-id')]	VLAN and Network IDs are optional. They are appropriate for inventory-items.
Any Inventory	System Administrator/ Owner	Name of the system administrator or owner.	uuid (of valid Party)	Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	software	Yes	"asset-owner" or "asset-administrator" role	1+	Error	context="//inventory-item[../../system-characteristics/security-sensitivity-level/text()='fips-199-high']" target="./ (./responsible-party | //component[@uuid=./implemented-component/@component-uuid] /responsible-role)[@role-id=('asset-owner', 'asset-administrator')]" count(party[@uuid=./party-uuid]) >= 1	For HIGH-impact systems, every inventory-item MUST identify an asset-owner or administrator property either within the inventory-item itself, or within the component linked by the inventory-item. This information is preferred, but optional for Moderate, Low and LI-SaaS impact level systems.
Any Inventory	Application Administrator/ Owner	Name of the application administrator or owner.	uuid (of valid Party)	Optional for OS/Infrastructure. Leave blank for Containers, Software and Database.							
Any Inventory	Function	The function provided by the component for the system.	markup-multiline	Mandatory for all assets/components	software, hardware, service	Yes	"function" prop/remarks	1	Error	context="//inventory-item" target=". | //component[@uuid=./implemented-component/@component-uuid]" exists(./prop[@name='function']/remarks)	Every inventory-item MUST describe the function provided by the item, either within the inventory-item itself, or within the component linked by the inventory-item.

Any Inventory	End-of-Life	Date that asset is expected to reach end-of-life (EOL). Please ensure that you notify your AO if the initial date changes.	date	Mandatory for any OS/Infrastructure/ Container/Software and/or Database that will reach EOL.		Yes	"end-of-life-date" FRX	0 or1	none
									
									Enforce 'date' Data Type
										//inventory-item/prop[@name='end-of-life-date' @ns='http://fedramp.gov/ns/oscal']
										
										//component/prop[@name='end-of-life-date' @ns='http://fedramp.gov/ns/oscal']
										
										--- 	
										context="//(component | inventory-item)"
										
										<matches target="./prop[@name='end-of-life-date']/@value" datatype="date"/>
											Where applicable the end-of-life date must be provided; however, there is currently no way to write a constraint that detects whether this information is available for inclusion.
											
											In the future, we could potentially look up the software in a dabase that could tell us.
											
											Where the property is present, the 'date' datatype must be enforced.

FRX = FedRAMP Extension		GUIDANCE	Valid Values	Mandatory or Optional?	//component/@type (asset-type)	Inventory-Item	Field/Prop	Cardinality	Level	Metapath or Constraint	Notes

Any Inventory	Scan Type		"infrastructure", "database", "web", "other", "not-applicable"			Yes	"scan-type" FRX	1+	Error
									Allowed Values
									Error
										context="//inventory-item"
										
										target=". | //component[@uuid=./implemented-component/@component-uuid]"
										
										exists(./prop[@name='scan-type' @ns='http://fedramp.gov/ns/oscal'])
										
										--- 	
										
										target=". | //component[@uuid=./implemented-component/@component-uuid]/prop [@name='scan-type' @ns='http://fedramp.gov/ns/oscal']/@value"
										
										allow-others: No
										- infrastructure: this item is scanned with an infrastructure or operating vulnerability scanner
										- database: this item is scanned with a database vulnerability scanner
										- web: this item is scanned with a web vulnerability scanner
										- other: this item is scanned with a non-typical vulnerability scanner as described in the remarks
										- not-applicable: scanning does not apply to this item as justified in the remarks
										
										--- 	
										
										exists(target=". | //component[@uuid=./implemented-component/@component-uuid]/prop [@name='scan-type' @ns='http://fedramp.gov/ns/oscal' @value=('other', 'not-applicable')]/remarks"
										)
											Every inventory-item MUST indicate one or more scan type(s), either within the inventory-item itself, or within the component linked by the inventory-item.
											
											Allowed values must be enforced.
											
											If the provided value is 'other' or 'not-applicable' the remarks field must be present.

	FIPS 140-2 Validation		uuid or uri fragment		software, service	Yes	--	0+		//inventory-item/implemented-component/@component-uuid (UUID of "validation" component)
										
										//component[@type='software']/link[@rel='validation']/substring-after(@href, '#') (UUID of "validation" component)
											Where an inventory item makes use of a cryptographic module, the module MUST be FIPS-140-2 or -3 validated, as represented in a "validation" component. The validation component MUST be linked to the inventory item, either directly via an implemented-component/@component-uuid link or via a linked component.

		Any OSCAL inventory-item not associated with a component must have the "asset-type" property.					"asset-type" prop	1+	Error	context="//inventory-item[not(./implemented-component)]" target="." exists(./prop[@name='asset-type'])	