2022 IRDR Part Four
IT Inventory
Supplemental Instructions

Guidance for Texas State Agencies

<u>Submission Deadline, March 31, 2022</u>

Texas Department of Information Resources

Contents

Key Information

Background

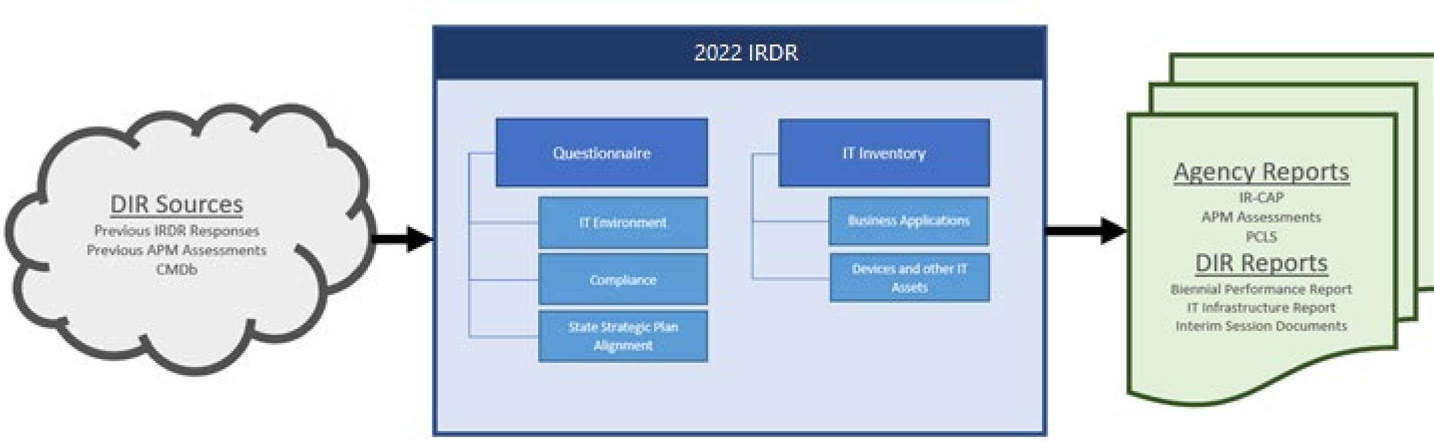
The Information Resources Manager (IRM) of each Texas state agency and institution of higher education (IHE) is required to conduct an IRDR every two years. DIR is providing Part 4 supplemental instructions to explain the inventory required under Texas Government Code, Sections 2054.068 and 2054.0965. Primarily, these instructions provide guidance on how to enter the information in the Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM).

DIR uses the information from this inventory to provide a statewide or enterprise perspective of information technology infrastructure and associated business applications used by state agencies. The inventory provides information for several required reports, including an assessment of security and operational risks.

DIR will prepopulate some information to ease the reporting burden for agencies. However, it is the agency’s responsibility to ensure that inventories are accurate and completed. DIR has added additional fields to provide agencies with more in-depth tools and the ability to track that information.

IHEs are not required to enter their inventory in SPECTRIM, but DIR highly encourages participation as this tool can help IHEs better manage their technology inventory and serve as a central repository.

Certain information concerning the vulnerability of systems collected for the purpose of 2054.068 will be treated as confidential through an exception granted on Chapter 552, Government Code. This includes the information collected in Part 4 – IT Inventory. The agency should take care to not provide system-comprising information in text-responses in the general IRDR. DIR will comply with the Texas Public Information Act for public information requests but will strive to ensure no system-comprising information is released in the process. Per Texas Government Code, section 552.139, Information is excepted from the requirements of Section 552.021 if it is information that relates to computer network security, to restricted information under Section 2059.055, or to the design, operation, or defense of a computer network.



Reporting Overview

Getting Started

Overview

DIR is required to conduct an inventory of each state agency's information technology infrastructure, including agency servers, mainframes, major databases, cloud services (collected as part of the Business Applications inventory), managed infrastructure, and other IT equipment. In SPECTRIM, this “inventory” is collected in the “Devices “and “Applications” modules.

Devices

- Agencies must review and update the devices inventory list to ensure it is complete and add any NEW devices or other IT assets or items that are outside of the scope of Data Center Services (DCS).
- There are several input fields shown, but not all information is required. Some fields are optional or read only. Required fields are marked with a red asterisk.
- It is important to include criticality information including risk metrics, data types, and monitoring information for active application.
- Also, it important to associate devices to business applications to provide insight into the security posture and potential impacts of infrastructure changes on agency applications.

Applications

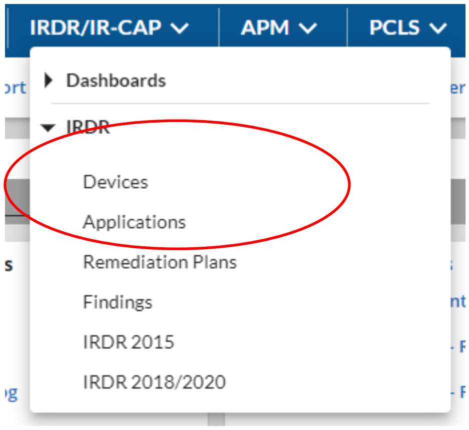
- The Applications Inventory application in SPECTRIM is a repository of all business applications used by the organization to perform business operations.
- Agencies must review and update the application inventory list to ensure it is complete and add any NEW application.
- There are several input fields shown, but not all information is required. Some fields are optional or read only. Required fields are marked with a red asterisk.

- Agencies have the option to generate a new Application Portfolio Management assessment (APM assessment) for that application.

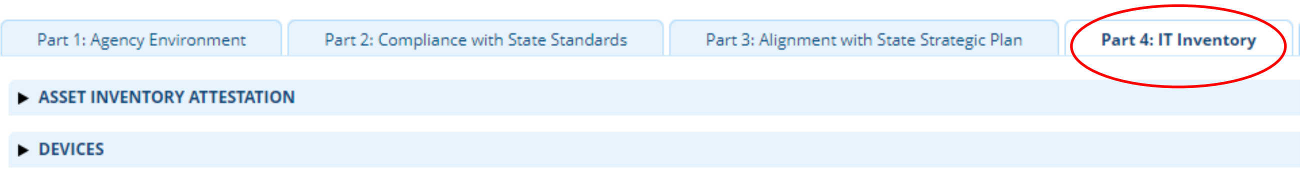
Reviewing and Adding a Record

There are two ways to review and update the inventory:

1. For an overview of all devices, select 'Devices' or 'Applications' from the IRDR menu at the top of the page. This method utilizes in-line edit (similar to an Excel document).

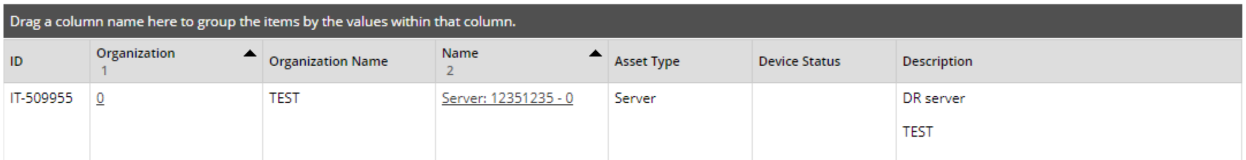


2. 'Devices' and 'Applications' can also be accessed from the IRDR itself by selecting the 'Part 4: IT Inventory' tab and expanding the 'Devices' or 'Applications' sub-sections.


Part 1: Agency Environment
Part 2: Compliance with State Standards
Part 3: Alignment with State Strategic Plan
Part 4: IT Inventory
ASSET INVENTORY ATTESTATION
DEVICES

Method 1: In-Line Editor

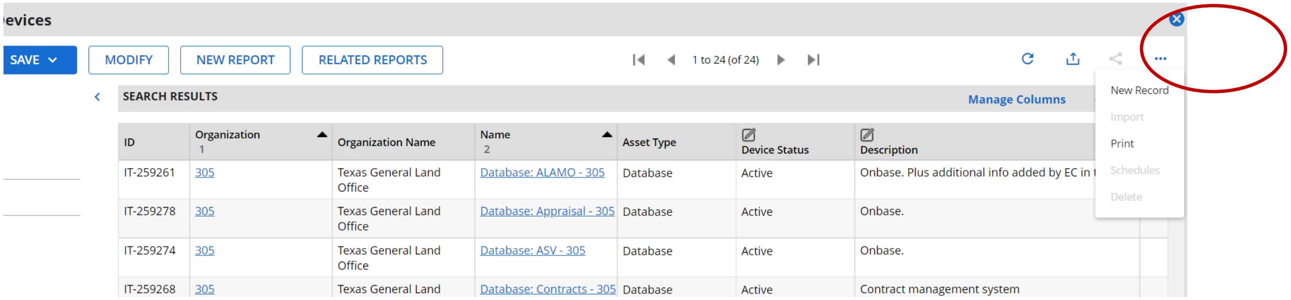
Selecting Devices or Applications takes you to the in-line editor which functions like Excel. It allows you to quickly make edits to certain fields. If you select the name of the device or application, it will open the individual editor where you can enter additional information.



Drag a column name here to group the items by the values within that column.

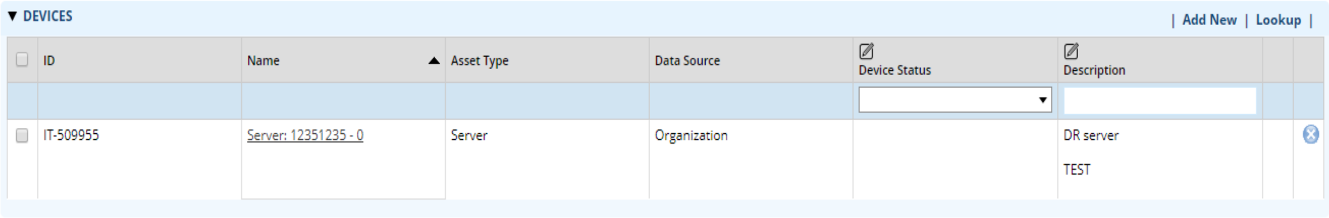
ID	Organization 1	Organization Name	Name 2	Asset Type	Device Status	Description
IT-509955	0	TEST	Server: 12351235 - 0	Server		DR server TEST

You can add a new device from in-line edit mode by selecting the drop down on the right-hand side.



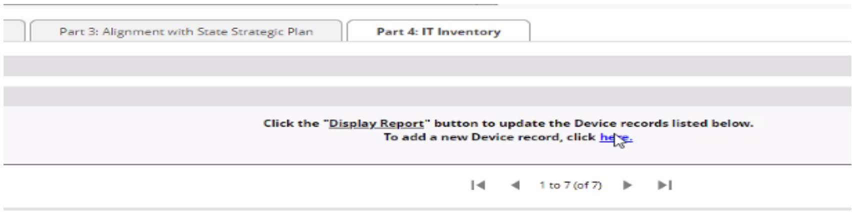
ID	Organization 1	Organization Name	Name 2	Asset Type	Device Status	Description
IT-259261	305	Texas General Land Office	Database: ALAMO - 305	Database	Active	Onbase. Plus additional info added by EC in t
IT-259278	305	Texas General Land Office	Database: Appraisal - 305	Database	Active	Onbase.
IT-259274	305	Texas General Land Office	Database: ASV - 305	Database	Active	Onbase.
IT-259268	305	Texas General Land	Database: Contracts - 305	Database	Active	Contract management system

Method 2: In IRDR Editor



□	ID	Name	Asset Type	Data Source	Device Status	Description
□	IT-509955	Server: 12351235 - 0	Server	Organization		DR server TEST

From the IT Inventory home section, expand the 'Devices' or 'Applications' sub sections. This will show a full list of all applications and devices that were carried over from the CMDb or from the previous IRDR.



Click the "Display Report" button to update the Device records listed below.
To add a new Device record, click here.

You can also add new devices and applications by using quick links from the IRDR dashboard to add a new record.

Devices and Other IT Assets Inventory

General Information

DIR is required to conduct an inventory of each state agency's information technology infrastructure, including agency servers, mainframes, major databases, cloud services (collected as part of the Business Applications inventory), managed infrastructure, and other IT equipment. In SPECTRIM, this inventory is collected in the 'Devices' and 'Applications' modules and includes devices as well other IT assets such as databases that are not business applications.

DIR has prepopulated inventory information from recent IRDRs and, for Data Center Services (DCS) agencies, some information from the Shared Technology Services CMDb server, network gear, and mainframe inventory.

Agencies must review the devices inventory list to ensure it is complete and add any NEW devices or other IT assets or items that are *outside of the scope of DCS;* please change the status for retired and duplicate devices or other IT assets.

Include as much additional detail as possible; new fields have been added to include the Asset Value, Device Role, Deployment Location, Technology Details, Related Applications, Risk Metrics, and Monitoring Details.

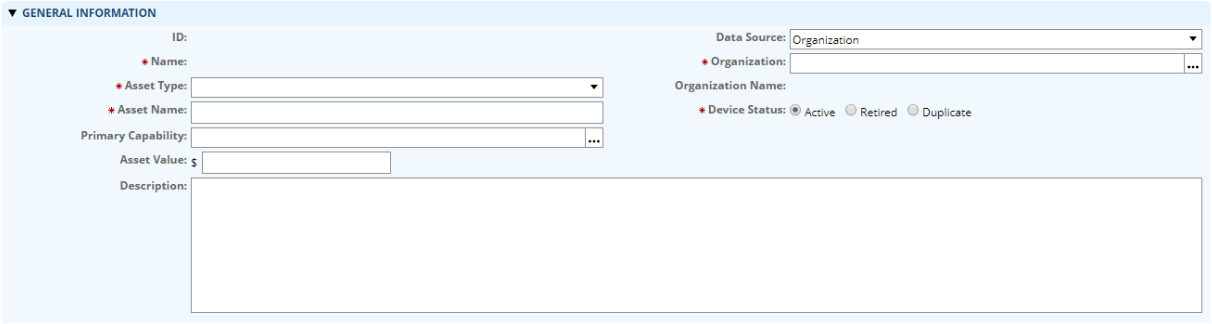
After you complete the update of your inventory, be sure to certify that all agency assets and applications are listed in SPECTRIM by checking the CONFIRMED box in the 2022 attestation section.

Required Fields

The General Information section contains most of the required fields. These include:

- Asset Name
- Asset Type
- Organization
- Device Status

Many of the input fields shown are optional for agencies to complete but are encouraged as doing so can help the agency with planning. Some fields may not be applicable for a given asset type. As a reminder, many of the fields will be prepopulated from previous IRDRs or from the CMDb.



▼ GENERAL INFORMATION

ID:

* Name:

* Asset Type:

* Asset Name:

Primary Capability:

Asset Value: $

Description:

Data Source: Organization

* Organization:

Organization Name:

* Device Status: ● Active ○ Retired ○ Duplicate

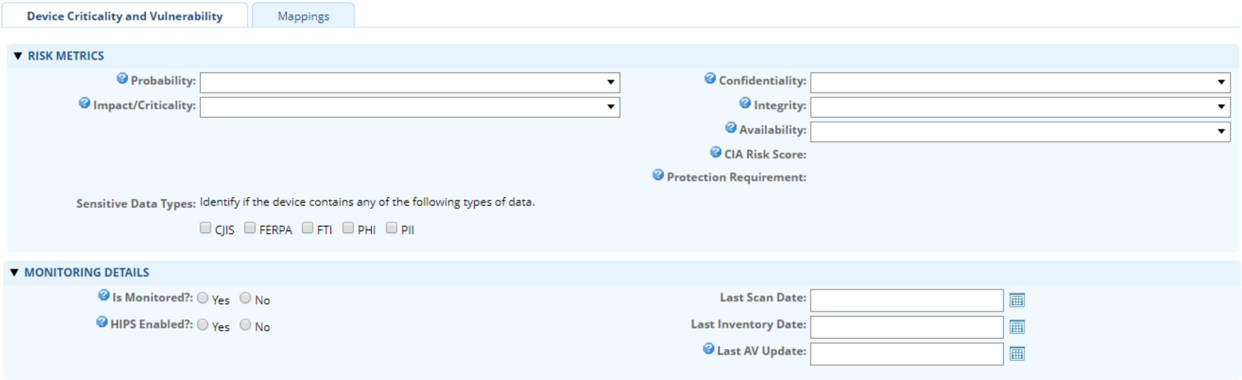
- A/V Equipment
- Database
- Firewall
- Hardware
- Load Balancer

- Mainframe
- Network Storage Device
- Other Network Asset
- Printer
- Router
- Security Device
- Server
- Storage Sever
- Switch
- Workstation

While there are several types of assets available for agencies to select, agencies are not *required to* report on all of them all. Agencies are only required to report on servers, mainframes, cloud services (part of the Business Application Inventory), and other information technology equipment.

Device Criticality and Vulnerability

While not required, it is important to include information on risk metrics. Responses to these questions will help to generate your risk score for the asset.



Device Criticality and Vulnerability | Mappings

▼ RISK METRICS

Probability:

Impact/Criticality:

Confidentiality:

Integrity:

Availability:

CIA Risk Score:

Protection Requirement:

Sensitive Data Types: Identify if the device contains any of the following types of data.

□ CJIS □ FERPA □ FTI □ PHI □ PII

▼ MONITORING DETAILS

Is Monitored?: ○ Yes ○ No

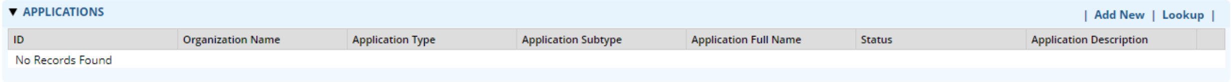
HIPS Enabled?: ○ Yes ○ No

Last Scan Date:

Last Inventory Date:

Last AV Update:

Associating Applications



▼ APPLICATIONS | Add New | Lookup |

ID	Organization Name	Application Type	Application Subtype	Application Full Name	Status	Application Description
No Records Found						

It is important to associate the agency's business applications with agency devices. If the associated application you are attempting to link to is not in the lookup field, then you can either add the application by clicking "Add New" or you can add the application later and link the devices from the application record. To do so, navigate to the 'Applications' sub-heading on the device you wish to associate with an inventoried device. From there you will need to select 'Look up' to generate a list of business applications, then select all applications associated with that device. By doing so, this provides agencies with a wholistic view of how their applications are mapped to servers and locations.

Associating devices to business applications can provide insight into the security posture and potential impacts of infrastructure changes on agency applications.

Business Applications Inventory

General Information

Business Applications Inventory

A Business Application name is the high-level label used by an agency business and IT organization to identify a group of functions provided by one or more systems to accomplish the specific business needs of the agency. A Business Application is typically a combination of integrated hardware and software (including data and applications), internally developed custom systems, commercial off the shelf (COTS) applications, and/or customized third-party systems.

The Applications Inventory application in SPECTRIM is a repository of all business applications used by the organization to perform business operations. Examples of applications include payment intake systems and customer information systems.

Organizations can use this feature to: track risk rating, business impact, licensing details, and personnel for various applications; identify risk vulnerabilities; map related software applications to the business processes they support; and classify and prioritize applications based on their value and criticality.

In Part 4 of the IRDR, DIR requires state agencies to validate the accuracy of the information about their business applications in SPECTRIM.

Business Applications Validation

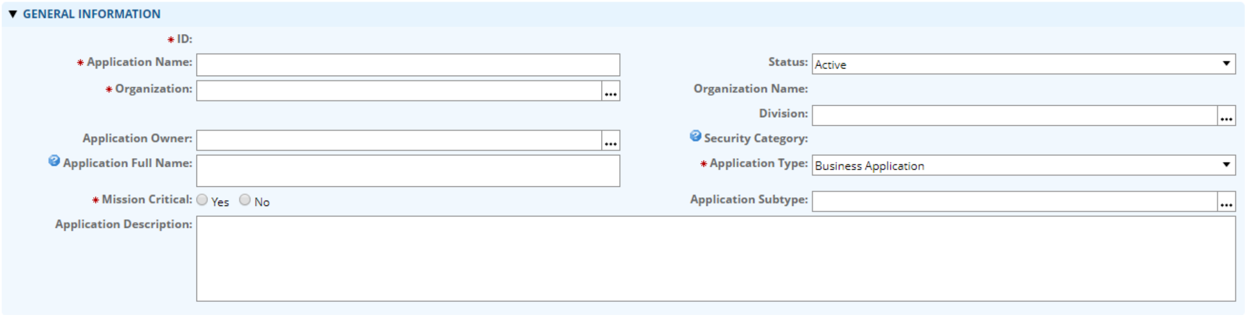
Application validation provides an updated list of agency business applications to link to your Device Inventory. It assists with the Prioritization of Cybersecurity and Legacy Systems (PCLS) Projects required by Section 2054.069.

Business applications will be required to have a current and accurate APM assessment completed in SPECTRIM in order to be included in PCLS project funding requests. Business applications that have been previously added in the SPECTRIM portal (previous IRDRs) are included in the inventory; within the application records, the agency can make the determination of whether to generate a new Application Portfolio Management assessment (APM assessment) for that application.

Once all applicable business applications have been entered and reviewed, agencies will need to check the CONFIRMED box within the business application attestation section on the Part 4: IT Inventory tab within the IRDR questionnaire.

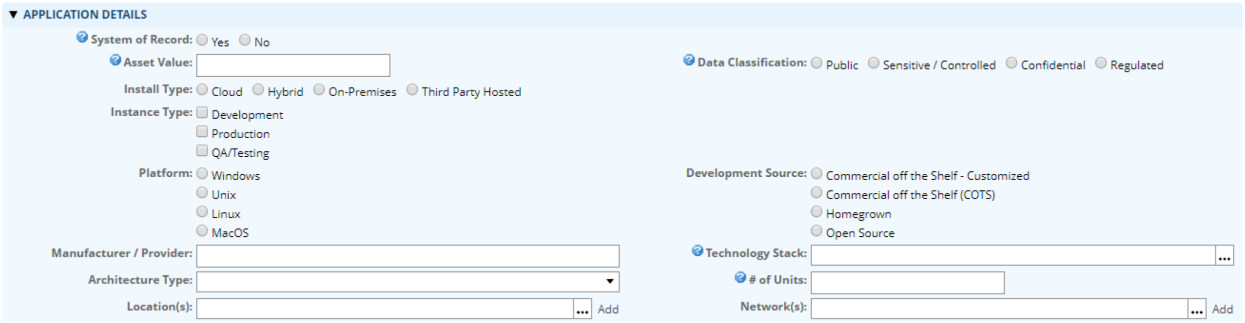
Reviewing Business Applications

Agencies should review the existing business applications and ensure the details and status of the applications are accurate.



▼ GENERAL INFORMATION

* ID:			
* Application Name:		Status:	Active
* Organization:		Organization Name:	
		Division:	
Application Owner:		Security Category:	
Application Full Name:		* Application Type:	Business Application
* Mission Critical:	○ Yes ○ No	Application Subtype:	
Application Description:			



▼ APPLICATION DETAILS

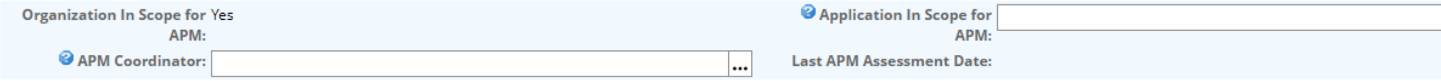
System of Record:	○ Yes ○ No		
Asset Value:		Data Classification:	○ Public ○ Sensitive / Controlled ○ Confidential ○ Regulated
Install Type:	○ Cloud ○ Hybrid ○ On-Premises ○ Third Party Hosted		
Instance Type:	□ Development □ Production □ QA/Testing		
Platform:	○ Windows ○ Unix ○ Linux ○ MacOS	Development Source:	○ Commercial off the Shelf - Customized ○ Commercial off the Shelf (COTS) ○ Homegrown ○ Open Source
Manufacturer / Provider:		Technology Stack:	
Architecture Type:		# of Units:	
Location(s):	Add	Network(s):	Add

Required Information

As with the devices inventory, the General Information section contains most of the required fields. For business applications, this includes:

- Name
- In Scope for APM
- Generate New Assessment
- Application Owner
- Mission Criticality

In Scope for APM & Generate New APM Assessment

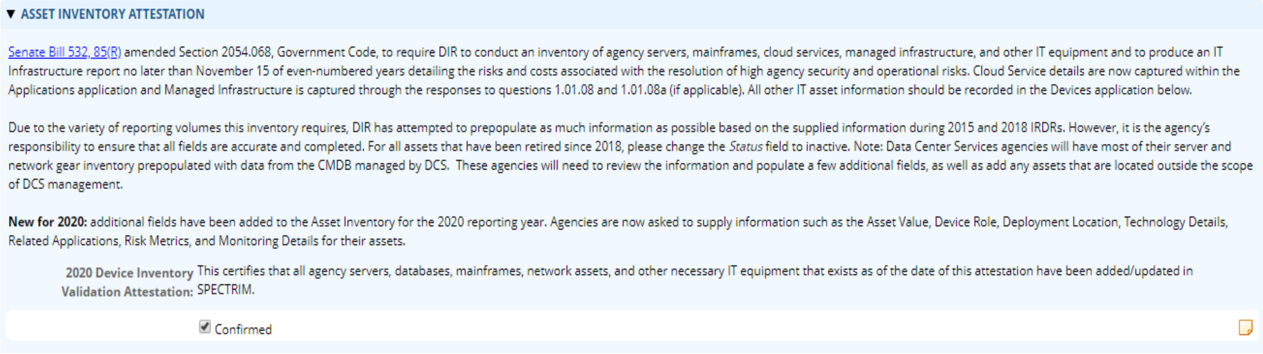


Organization In Scope for APM:	Yes	Application In Scope for APM:	
APM Coordinator:		Last APM Assessment Date:	

If an agency would like to complete an APM assessment on the application, then select "Generate New APM Assessment."

A current and accurate APM assessment is required for PCLS questionnaire submission. Agencies can view previous APM assessments and application risk assessments within the respective sections in the application record by clicking on the hyperlinked key field of those records.

Attestation and Completion



▼ ASSET INVENTORY ATTESTATION

Senate Bill 532, 85(R) amended Section 2054.068, Government Code, to require DIR to conduct an inventory of agency servers, mainframes, cloud services, managed infrastructure, and other IT equipment and to produce an IT Infrastructure report no later than November 15 of even-numbered years detailing the risks and costs associated with the resolution of high agency security and operational risks. Cloud Service details are now captured within the Applications application and Managed Infrastructure is captured through the responses to questions 1.01.08 and 1.01.08a (if applicable). All other IT asset information should be recorded in the Devices application below.

Due to the variety of reporting volumes this inventory requires, DIR has attempted to prepopulate as much information as possible based on the supplied information during 2015 and 2018 IRDRs. However, it is the agency's responsibility to ensure that all fields are accurate and completed. For all assets that have been retired since 2018, please change the *Status* field to inactive. Note: Data Center Services agencies will have most of their server and network gear inventory prepopulated with data from the CMDB managed by DCS. These agencies will need to review the information and populate a few additional fields, as well as add any assets that are located outside the scope of DCS management.

New for 2020: additional fields have been added to the Asset Inventory for the 2020 reporting year. Agencies are now asked to supply information such as the Asset Value, Device Role, Deployment Location, Technology Details, Related Applications, Risk Metrics, and Monitoring Details for their assets.

2020 Device Inventory Validation Attestation: This certifies that all agency servers, databases, mainframes, network assets, and other necessary IT equipment that exists as of the date of this attestation have been added/updated in SPECTRIM.

☑ Confirmed

Once both sections are confirmed the inventory portion of the IRDR is complete. After saving the questionnaire, the part 4 progress indicators will change to green check marks.

If you have any questions about the content of this document, please email irdr@dir.texas.gov.