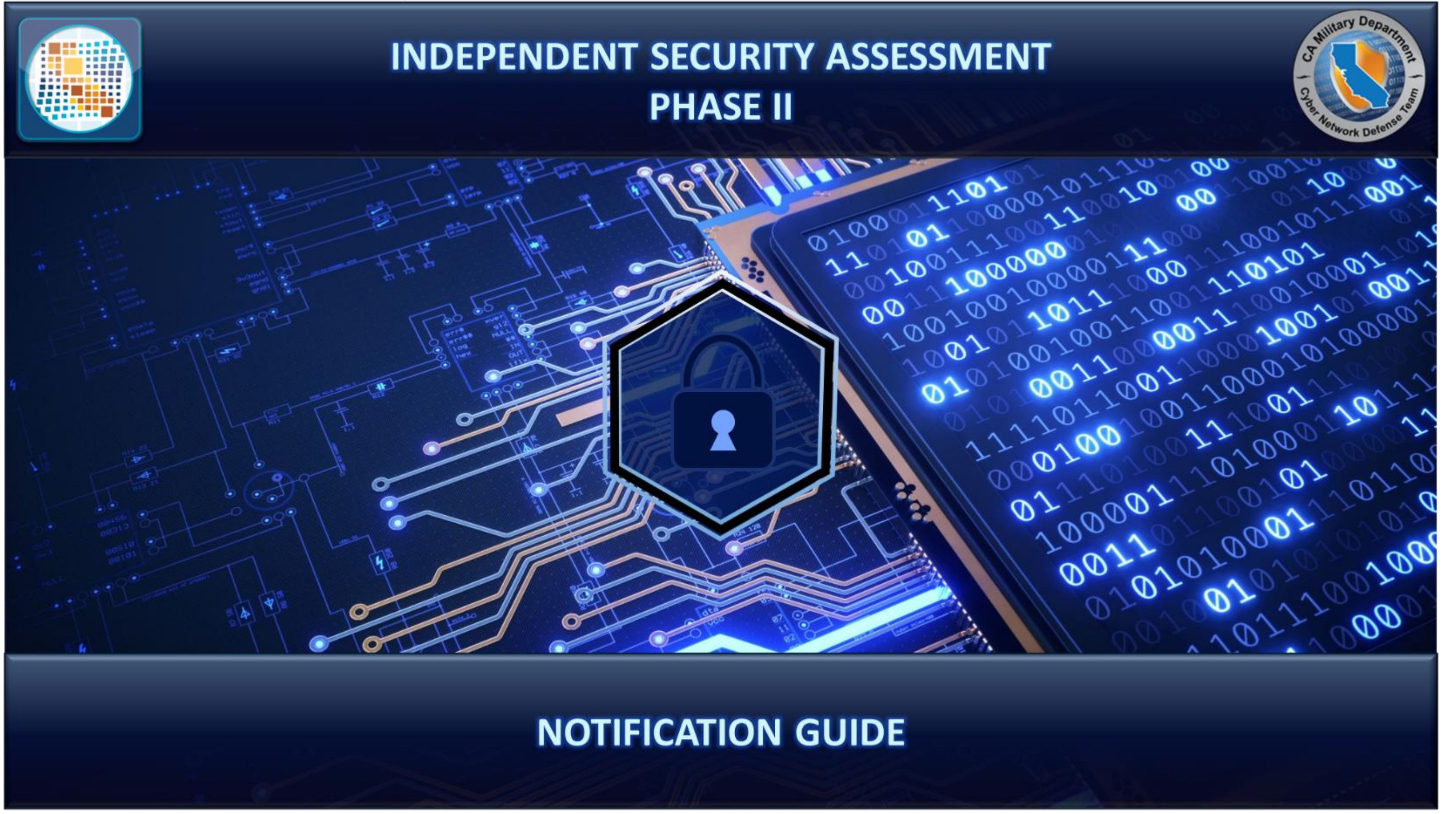
California
DEPARTMENT OF TECHNOLOGY
Office of Information Security

Provided By

California Military Department
Cyber Network Defense



INDEPENDENT SECURITY ASSESSMENT
PHASE II

NOTIFICATION GUIDE

Instructions for Assessed Entities

Actions Required Upon Notification
Timelines for Completion

Version 5.1
3/11/2021
Previous editions are obsolete

Table of Contents

Independent Security Assessment (ISA) Overview

The Independent Security Assessment (ISA), sometimes referred to as an AB 670 Assessment, is required by California Government Code section 11549.3 as amended January 1, 2016. The ISA is a technical assessment of a state entity's network and selected web applications, to identify security vulnerabilities and provide concrete, implementable actions to reduce the possibility of damaging security breaches. The ISA utilizes a series of technical controls based on NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations" and the State Administrative Manual (SAM), Chapter 5300 "Information Security" as selected by the California Department of Technology (CDT) Office of Information Security (OIS). Under GC 11549.3, state entities, as defined by Government Code 11546.1, receive an ISA every other year. ISAs have been incorporated into the continuous Oversight Lifecycle, which consists of a full audit, check-in audit, and two ISAs over a period of multiple years. ISAs are performed either by the California Military Department (CMD), Cyber Network Defense (CND) unit or by a 3rd party upon the approval of OIS. Entities are assessed either by receiving a CND ISA or contracting for a 3rd party ISA.

This Notification Guide is intended to ensure the ISA is conducted efficiently, with minimum impact to state entities. It is important to review this Guide in its entirety to be fully prepared for the ISA and derive the maximum benefit from it.

Notification Process

Entities begin the ISA process when they receive a formal notification letter from CDT OIS advising them that it is their year to undergo an ISA. Upon receipt of this formal notification letter, the entity must complete one of the following actions: **Schedule ISA-** Open an ISA request from the CDT IT Service Management Portal (also known as "ServiceNow") Service Catalog (see Appendix A for instructions) within thirty business days of the date of notification or **Request Waiver** within twenty business days of the date of notification**.** These actions are explained in the table below:

Schedule ISA	Request Waiver	
Open an ISA request from the CDT IT Service Management Portal (also known as "ServiceNow") Service Catalog (see Appendix B for instructions).	Contact OIS to request an **ISA Compliance Certification Form.** Waivers are permitted for two specific reasons only:	
	Host / Hosted Condition: The entity is included within a single Host entity, as reported previously to OIS. In this situation, the Hosted entity should be assessed at the time their Host entity is assessed.	**3rd Party Provider:** Entity seeks approval to undergo a commercial, 3rd party ISA. The entity must attach a copy of the proposed Statement of Work for the contract to the Form. The completed ISA report must meet the ISA Criteria* **EXACTLY** and follow the SAME FORMAT as the criteria or it will be rejected.

* The ISA Criteria can be obtained through your entity's designated ISO.

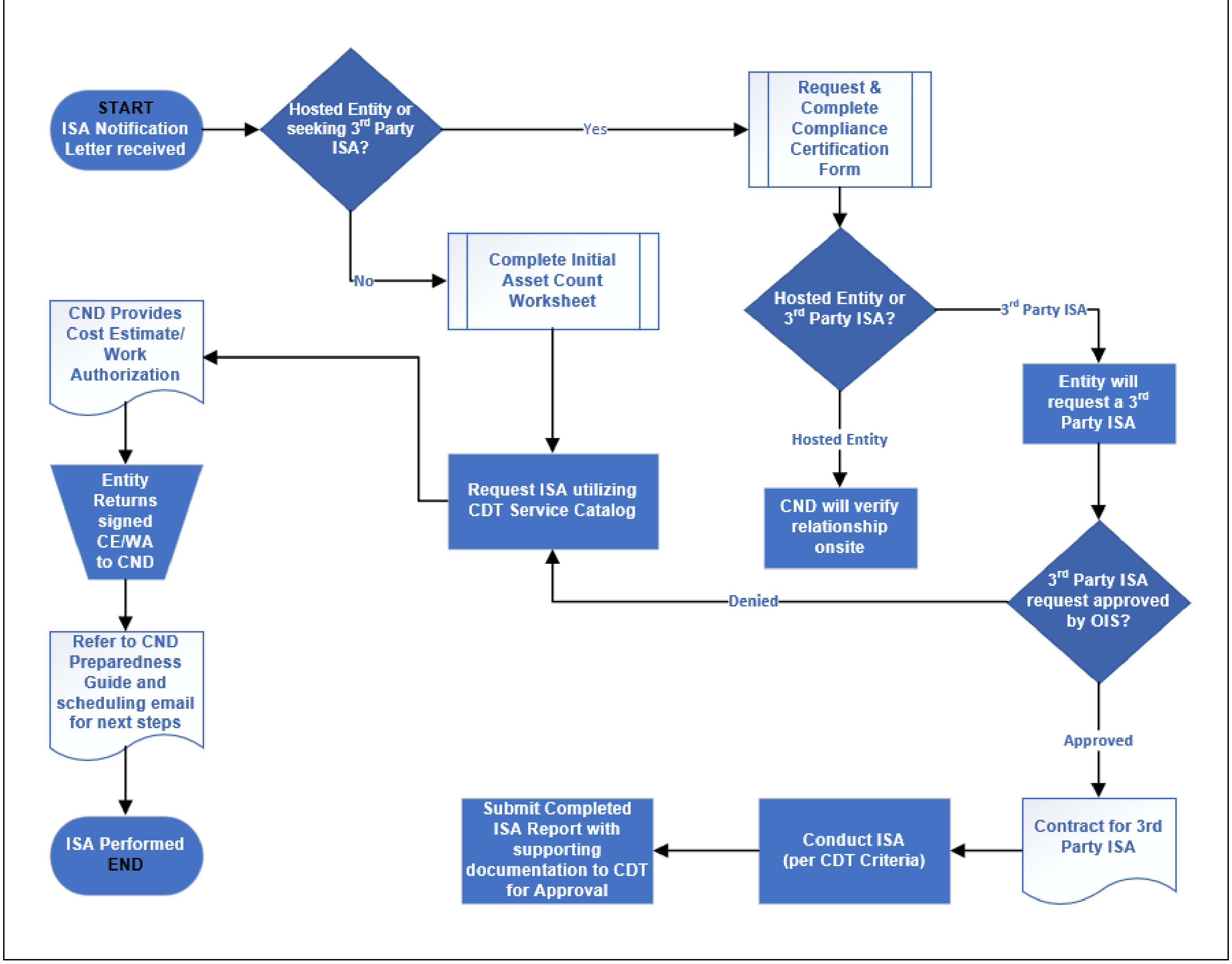
Distributing the Notification Guide

The Notification Guide is designed to help the assessed entity coordinate scheduling the ISA. It is critical this document be disseminated internally by the assessed entity to the responsible individuals within the organization who will be providing the data and support necessary to complete the notification process. The notification process must be completed within 30 business days of receiving the notification letter from CDT OIS. It is recommended that the entity's most *senior manager responsible for cybersecurity* (e.g., AISO, CISO or CIO) manage the efforts detailed in this Guide. Late scheduling may result in non-compliance reporting to OIS and their stakeholders, including the Department of Finance and the Governor's Office.

Preparing for the ISA

This Guide is designed to assist the entity's Cybersecurity, Systems and Network teams through the coordination process.

Preparation Workflow


START
ISA Notification Letter received
Hosted Entity or seeking 3rd Party ISA?
Yes
Request & Complete Compliance Certification Form
No
Complete Initial Asset Count Worksheet
Hosted Entity or 3rd Party ISA?
3rd Party ISA
Entity will request a 3rd Party ISA
Hosted Entity
CND will verify relationship onsite
CND Provides Cost Estimate/ Work Authorization
Request ISA utilizing CDT Service Catalog
Entity Returns signed CE/WA to CND
3rd Party ISA request approved by OIS?
Denied
Approved
Refer to CND Preparedness Guide and scheduling email for next steps
ISA Performed
END
Submit Completed ISA Report with supporting documentation to CDT for Approval
Conduct ISA (per CDT Criteria)
Contract for 3rd Party ISA

Steps for Scheduling the ISA

The steps below align with the left side of the Preparation Workflow on the previous page. The steps are listed in the order they are to be completed, as soon as possible after receipt of the notification letter. Due to the compressed timeline involved in scheduling ISAs, concurrent execution of some of the steps may be helpful. If the entity is an existing CDT customer, a ServiceNow account is already established, and the same account should be used to create the ISA Case through the IT Service Portal. If the entity is not a CDT customer, they must contact Customer Engagement Services to obtain a ServiceNow account.

Steps 1 and 2 should be performed concurrently in accordance with the prescribed timeline on the Notification letter.

Step 1: Complete Initial Asset Count Worksheet

To begin the scheduling process, an initial asset count worksheet with an estimate of the number of hosts/assets that will be assessed during the ISA must be completed. The Initial Asset Count worksheet is a required attachment for requesting an ISA through the CDT IT services catalog. See Appendix A for the sample worksheet and instructions on completing the asset count. ***Note: Do not upload Data Call Worksheet to new or existing ISA ServiceNow cases.***

Step 2: Request an ISA from the CDT Service Catalog

Create the ISA Case from the CDT IT Services Portal catalog (also known as “ServiceNow”).
Once the ISA request is submitted, a Case number will be generated. The Case must be initiated within 30 days of the date of official notification (see Appendix B for instructions on accessing ServiceNow). The Case number will be provided to the CND Engagement Manager in order to obtain a cost estimate for the ISA. If assistance is required, the entity may contact their CDT Account Lead and ask for ISA Service Request assistance or call the CDT Service Desk at (916) 464-4311.

Step 3: Receive Confirmation of ISA Dates and Cost Estimate/Work Authorization

OIS will provide the entity’s ServiceNow Case number and Initial Asset Count worksheet to the CND. The entity will be contacted directly by the CND Engagement Manager to confirm the scheduled dates and asset count numbers. The Cost Estimate/Work Authorization (CE/WA) will be provided via email to the entity. The CE/WA will be based off the asset count provided by the entity.

Step 4: Return Cost Estimate/Work Authorization to CND, Lock in Assessment Dates

The emailed CE/WA, summarizing the cost of the ISA, will be reviewed and signed by the entity’s ISO, CIO or other designee. The signed CE/WA is then returned to the CND Engagement Manager. Once CND receives the signed CE/WA, the entity’s assessment dates will be officially scheduled.

Step 5: Refer to CND Preparedness Guide

Upon completion of Step 4, the entity will receive a copy of the CND Preparedness Guide from the CND Engagement Manager with an email confirming the schedule for their ISA. The Preparedness Guide will enable the entity to be as prepared as possible for CND’s arrival on site and to ensure the best possible outcome and benefits from the ISA.

Requesting a Waiver

If CND is *not* performing the ISA, the entity must complete the ISA Compliance Certification Form which addresses the following two specific circumstances under which a waiver may potentially be allowed:

- **Entity is Hosted in a** Host/Hosted **Relationship (Previously referred to as the Parent/Child Relationship).** This will be based in accordance with the most recently submitted Designation Letter (SIMM 5330-A). In this case, the entity will be assessed when the Host is assessed.
- **3rd Party Provider:** The entity seeks approval to undergo a commercial, 3rd party ISA. The entity must include a copy of the proposed Statement of Work for the procurement. **The ISA and ISA report must meet CDT ISA criteria EXACTLY and follow the same format as the criteria or it will be rejected.**

Please note that approval of the ISA Compliance Certification Form is at the discretion of OIS and may or may not be granted. Contact OIS at security@state.ca.gov to request a copy of the form.

Waiver Request Cases

1. ISA Notification Received in Error

ISAs are completed on a bi-annual basis. Entities that have completed an approved ISA in the previous fiscal year, but still received formal notification that they are due for an ISA must take one of the following actions, depending on who performed the ISA:

- **CND performed the ISA:** Notify OIS of the issue via email immediately at security@state.ca.gov. The email should include the ISA ServiceNow Case number and date of the last ISA. No additional documentation is required, OIS will verify the information.

- **3rd Party ISA:** Notify OIS via email at security@state.ca.gov and arrange for a copy of the ISA and all supporting data/artifacts to be delivered to OIS (if this has not already been done).
    - OIS will review the ISA to determine whether the ISA Criteria was satisfied.
    - If OIS determines the ISA Criteria was not satisfied, the entity must either remediate and resubmit the ISA within 60 days or CND will perform an ISA in the following fiscal year.

2. Host / Hosted Status

OIS developed the Host/Hosted criteria so that entities sharing a logical security infrastructure can be considered as a single entity for Auditing and Assessment purposes. As stated in the OIS Designation Letter (SIMM 5330-A), the following criteria must be met for an entity to be considered a Child:

- The Hosted entity DOES NOT have a separate Active Directory from the Host, **and/or** has an Active Directory that is FULLY managed by the Host;
- The Hosted entity DOES NOT have a separate information security policy boundary from the Host; and
- The Hosted entity is ENTIRELY CONTAINED within the Host security boundary.

Under Host/Hosted, Hosted entities will be assessed at the time of the Host ISA. Effective January 2018, entities are required to identify their Host/Hosted status on the OIS Designation Letter which is due according to the schedule in the OIS Information Security Compliance Reporting Schedule (SIMM 5330-C) https://cdt.ca.gov/wp-content/uploads/2018/02/SIMM-5330_C.pdf. If the date for the Host ISA falls before the due date for the Designation Letter, the entity can complete the Compliance Certification form which requests the same information. (At a future date, the Compliance Certification form will be modified to reflect that this information is now captured in the Designation Letter.) If it is determined at the time of an assessment that the Hosted entity **does not meet ALL THREE of the criteria above**, the Hosted entity will still be assessed, and any amount billed or due will be direct billed to the designated Host entity.

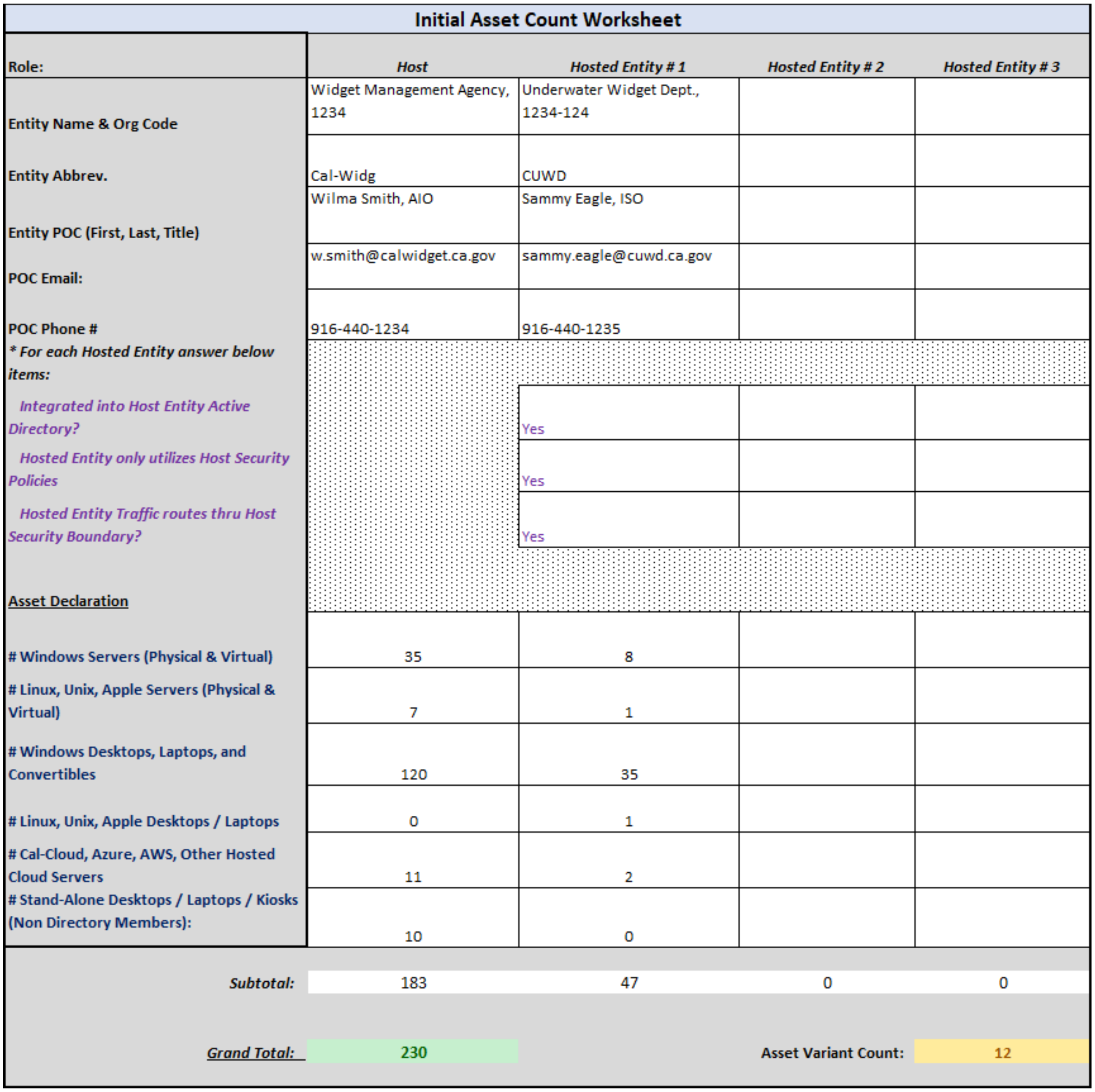
3. Third Party ISAs

Entities seeking the services of a commercial provider to perform the ISA must request and submit an **ISA Compliance Certification Form** to OIS within 20 days of ISA notification. The entity must attach a copy of the proposed Statement of Work to the Form. The ISA must meet the ISA criteria EXACTLY and follow the same format as the criteria or the ISA Report will be rejected.

Appendix A – Initial Asset Count Worksheet

Purpose: The purpose of this form is to estimate the number of hosts/assets that will be assessed during the Independent Security Assessment (ISA). For assessment purposes, a host/asset is considered in-scope if it meets one of the criteria listed on this form. List your assets using the classifications listed below. Be as accurate as possible as it affects both CND resource scheduling and the final cost of the ISA. If the actual asset count discovered exceeds 5% or more of the estimated count, the entity acknowledges additional costs may apply. The completed Initial Asset Count Worksheet will be attached to the ServiceNow Case. If you did not receive a copy of the Initial Asset Count Worksheet with your Notification Letter, email info@cnd.ca.gov.

Asset Estimation Example:



Initial Asset Count Worksheet

Role:	***Host***	***Hosted Entity # 1***	***Hosted Entity # 2***	***Hosted Entity # 3***
Entity Name & Org Code	Widget Management Agency, 1234	Underwater Widget Dept., 1234-124		
Entity Abbrev.	Cal-Widg	CUWD		
Entity POC (First, Last, Title)	Wilma Smith, AIO	Sammy Eagle, ISO		
POC Email:	w.smith@calwidget.ca.gov	sammy.eagle@cuwd.ca.gov		
POC Phone #	916-440-1234	916-440-1235		
**** For each Hosted Entity answer below items:***				
Integrated into Host Entity Active Directory?		Yes		
Hosted Entity only utilizes Host Security Policies		Yes		
Hosted Entity Traffic routes thru Host Security Boundary?		Yes		
Asset Declaration				
# Windows Servers (Physical & Virtual)	35	8		
# Linux, Unix, Apple Servers (Physical & Virtual)	7	1		
# Windows Desktops, Laptops, and Convertibles	120	35		
# Linux, Unix, Apple Desktops / Laptops	0	1		
# Cal-Cloud, Azure, AWS, Other Hosted Cloud Servers	11	2		
# Stand-Alone Desktops / Laptops / Kiosks (Non Directory Members):	10	0		
Subtotal:	183	47	0	0
Grand Total:	230		**Asset Variant Count:**	12

Required Actions upon Completion:

Open an ISA Case in ServiceNow and attach the completed Asset Count Worksheet to the request. A fillable Asset Count Worksheet copy will be provided electronically during the notification process.

Generalized Guidance for Asset Counts:

The following information is intended to assist the entity in completing the Initial Asset Count Worksheet. This is a general guideline and cannot account for unique, special systems, or co-managed assets. If you are hosting more than your organization in your data center or server facility, you may be eligible for Host / Hosted status. For an entity to be declared as a Hosted Entity, each Hosted Entity must be able to have a verified "Yes" response to the 3 hosted criteria questions (purple text). "Yes" responses will be validated by CND at the beginning of your ISA. If additional clarification is needed, please contact the CND Engagement Manager at info@cnd.ca.gov.

- For each eligible Hosted Entity, list them in the applicable Hosted entity column and complete all required data.
- If you do not have any Hosted Entities, only complete the Host column.

Roles:

- **Entity Name and Org Code:** Enter the formal Name of your Organization and Org Code (e.g., Government Operations Agency, 7100)
- **Entity Abbrev:** Enter the formal organization abbreviation (e.g., GovOps)
- **Entity POC:** Enter the first, last and abbreviated title of the primary point of contact for questions regarding the data contained on this form.
- **POC Email:** Enter the official email address of the applicable entity Point of Contact.
- **POC Phone #:** Enter the official phone number for the applicable entity Point of Contact.

Hosted Entity Validation:

- **Integrated into Host AD:** Are the user and computer accounts objects within the Host's Active Directory?
- **Host Security Policies:** All security policies of the Host entity are logically enforced on all hosted entities / assets?
- **Security Boundary Routed Traffic:** All Hosted traffic is routed through and inspected by applicable Host IDS/IPS and Firewalls?

Asset Declaration:

- **# Windows Servers (Phy/VM):** Total number of Windows server operating system hosts. This includes Physical and virtual hosts that are not Cloud Hosted (e.g., Azure AD).
- **# Linux, Unix, Apple Servers (Phy/VM):** Total number of Windows server operating system hosts. This includes Physical and virtual hosts that are not Cloud Hosted (e.g., Mainframes, Mini-mainframes, Ubuntu, etc.…).
- **# Windows Desktop/Laptop/Convertibles:** Total number of Windows, non-server operating system hosts. This includes VDI host instances not externally Hosted (e.g., Citrix VDI internal server).
- **# Linux, Unix, Apple Desktops/Laptops:** Total number of non-windows, non-server operating system hosts. (e.g., Apple Laptops, Linux Desktops, Chromebooks, etc.….).
- **# Cal-Cloud, Azure, AWS, Other Hosted Cloud Svrs:** All hosts operated from an external data center, where entity has more than application-level access (e.g., Cal-cloud web servers, Azure DC's, AWS Database Servers, etc.…).
- **# Stand-Alone Desktops/Laptops/Kiosks (Non-Directory Members):** Hosts, not joined to the entities Active Directory connected to entity managed IP address space (e.g., Public Kiosks, IP Addressable Postal Meters, HVAC controllers, etc.…).

Totals:

- **Grand Total:** Total Assets used to calculate the time, labor and Operations and Maintenance expenses for process in the entity organization(s) listed.
- **Asset Variant Count:** The number of additional assets, above the number identified in the Grand Total that CND will process at no charge.

Assets Exempt from Categorization:

As a general rule, do ***not*** count:

- Routers, switches, VoIP telephones, Mobile Phones, Android / Apple Tablets, Modbus and other related SCADA class devices (not classified as IoT)
- 3rd Party devices residing on vendor controlled and isolated LAN segments (e.g., DSL line direct to HVAC)
- Microsoft Azure cloud email servers
- Telco Provider Sensors such as IPS/IDP collectors (not managed by entity)
- CDT/Cal-CSIC provided cybersecurity sensors/collectors

Scoping Clarification:

All assets included in the Asset Estimation section are subject to a vulnerability scan. Failure to identify all eligible assets could result in the ISA being declared invalid.

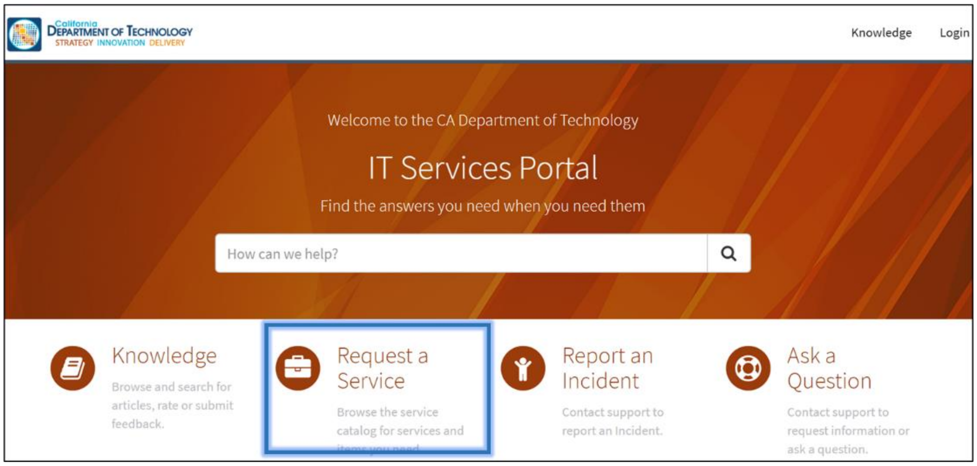
Appendix B – ISA ServiceNow Procedure

Purpose: This appendix is provided as a guide for completing the ISA Service Request (Case) in CDT's IT Services Portal (ServiceNow). A ServiceNow Case must be submitted within 30 business days of ISA notification. Once a Case has been submitted, no edits can be made to the initial request. If you have questions, please contact your CDT Account Lead.

1. You must have a completed copy of the Asset Count Worksheet in order to open a ServiceNow Case. Refer to Appendix A for instructions required to complete the worksheet.

2. Go to the IT Services Portal https://services.cdt.ca.gov/csm.

3. Select "Request a Service".



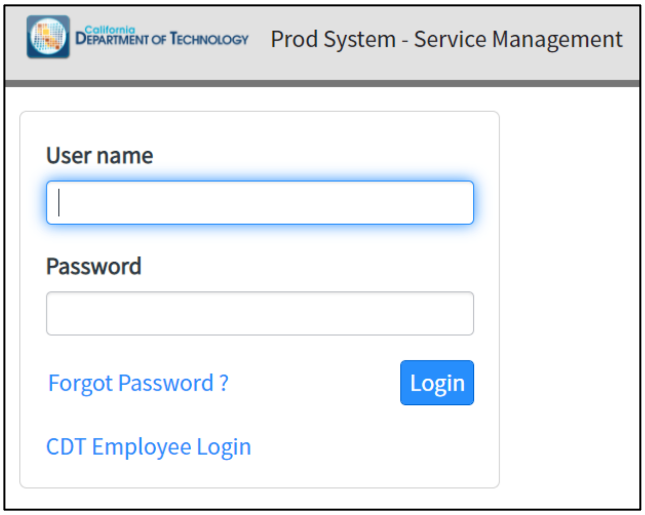
Welcome to the CA Department of Technology

IT Services Portal

Find the answers you need when you need them

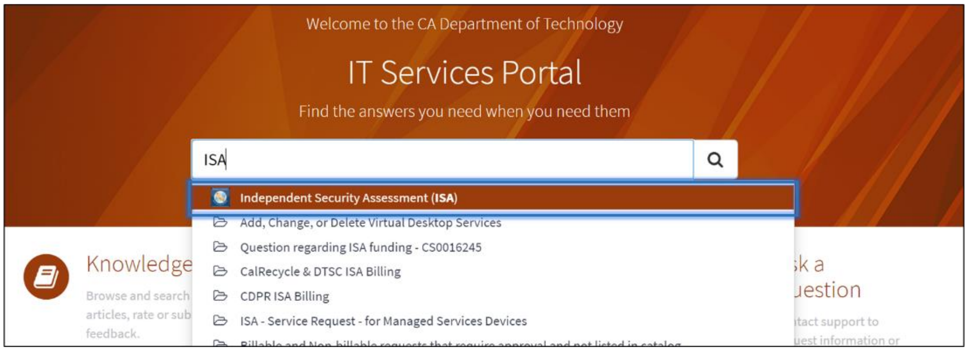
California Department of Technology
STRATEGY INNOVATION DELIVERY
Knowledge
Login
How can we help?
Knowledge
Browse and search for articles, rate or submit feedback.
Request a Service
Browse the service catalog for services and items you need
Report an Incident
Contact support to report an incident.
Ask a Question
Contact support to request information or ask a question.

4. When prompted, enter your ServiceNow User name and Password and select "Login". If you do not have a ServiceNow account, please contact your Account Lead or Customer Engagement Services at (916) 431-5390 for assistance.



California Department of Technology
Prod System - Service Management
User name
Password
Forgot Password ?
Login
CDT Employee Login

5. Once logged in, type “**ISA**” in search bar and select “Independent Security Assessment (ISA)” from the drop down menu.



Welcome to the CA Department of Technology

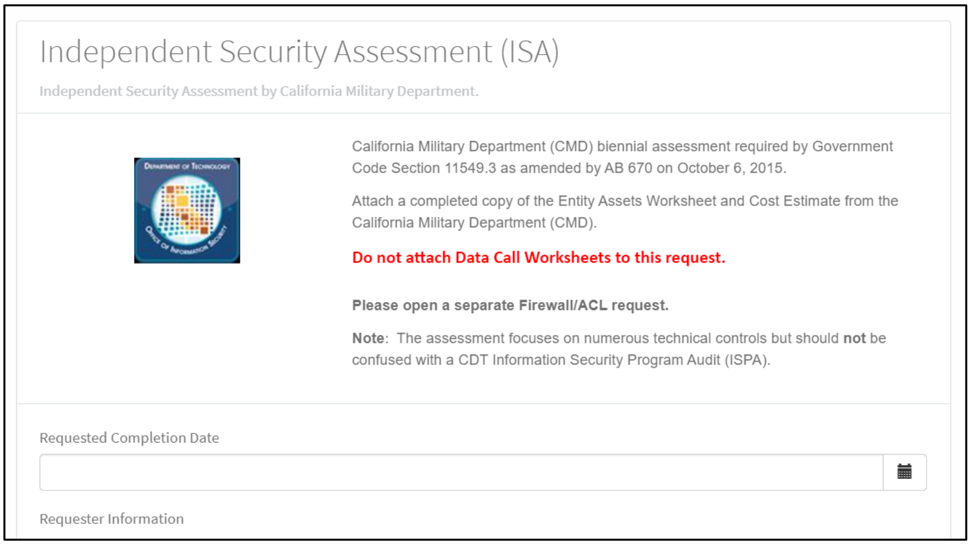
IT Services Portal

Find the answers you need when you need them

ISA

Independent Security Assessment (ISA)
Add, Change, or Delete Virtual Desktop Services
Question regarding ISA funding - CS0016245
CalRecycle & DTSC ISA Billing
CDPR ISA Billing
ISA - Service Request - for Managed Services Devices
Billable and Non-billable requests that require approval and not listed in catalog
Knowledge
Browse and search articles, rate or sub feedback.
sk a uestion
tact support to uest information or

6. Enter Requested Completion Date (Optional Field). We recommend you put the end of the Fiscal Year, i.e. 2022-06-30.



Independent Security Assessment (ISA)

Independent Security Assessment by California Military Department.

California Military Department (CMD) biennial assessment required by Government Code Section 11549.3 as amended by AB 670 on October 6, 2015.

Attach a completed copy of the Entity Assets Worksheet and Cost Estimate from the California Military Department (CMD).

Do not attach Data Call Worksheets to this request.

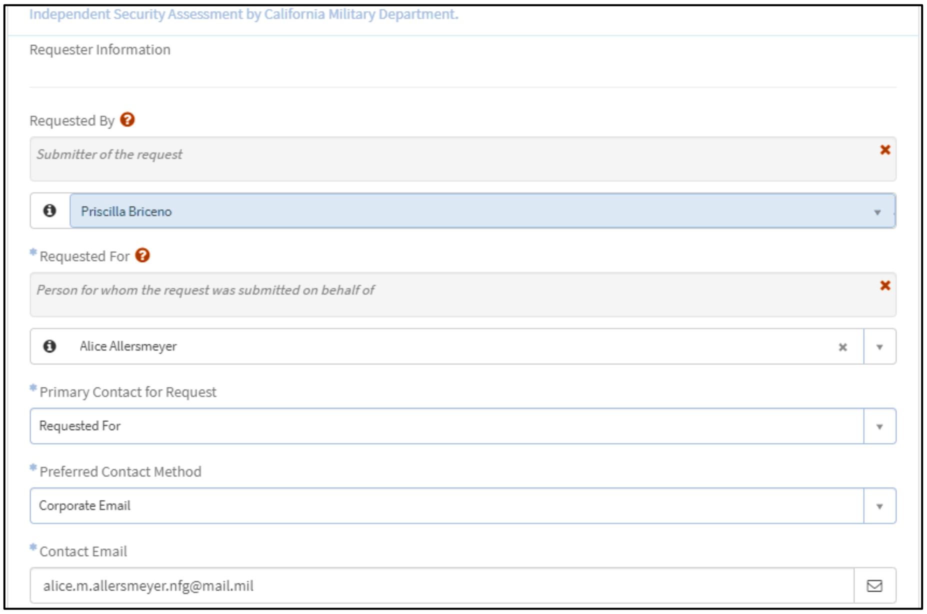
Please open a separate Firewall/ACL request.

Note: The assessment focuses on numerous technical controls but should **not** be confused with a CDT Information Security Program Audit (ISPA).

Requested Completion Date

Requester Information

7. Complete all requestor information. If the ‘Requested By” person is not the primary contact for the ISA, select “Requested For” in the “Primary Contact for Request” field.



Independent Security Assessment by California Military Department.

Requester Information

Requested By

Submitter of the request

Priscilla Briceno

*Requested For

Person for whom the request was submitted on behalf of

Alice Allersmeyer

*Primary Contact for Request

Requested For

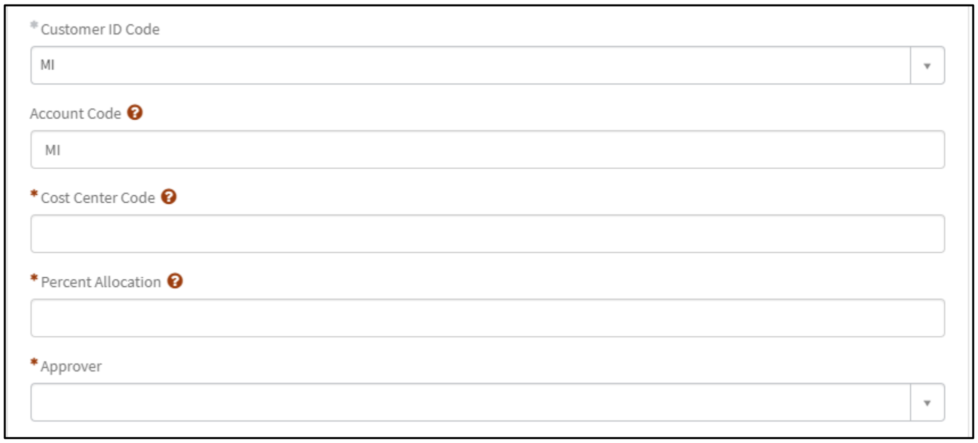
*Preferred Contact Method

Corporate Email

*Contact Email

alice.m.allersmeyer.nfg@mail.mil

8. Complete all fields that have an asterisk (*). Contact Account Lead for assistance with Account Codes and Cost Center Codes.



*Customer ID Code

MI

Account Code

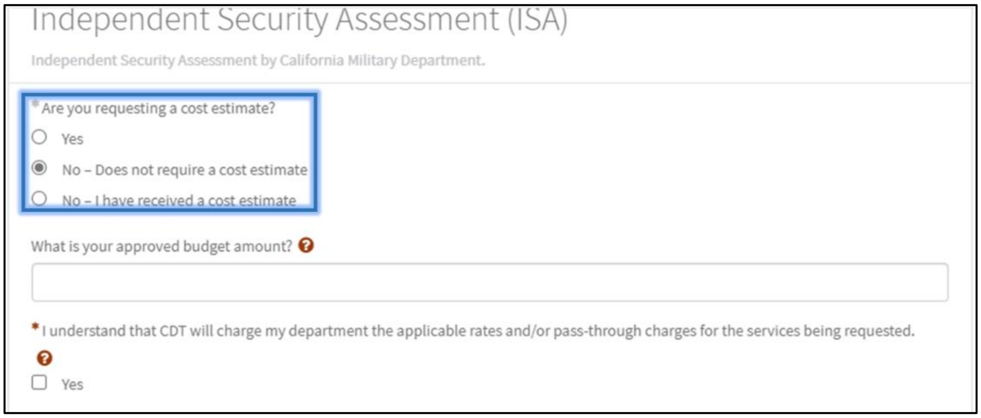
MI

*Cost Center Code

*Percent Allocation

*Approver

9. Select “No- Does not require a cost estimate”, or if you already have a cost estimate, select “No- I have received a cost estimate”. <u>Note:</u> Cost estimate will be provided by CND Engagement Manager.



Independent Security Assessment (ISA)

Independent Security Assessment by California Military Department.

*Are you requesting a cost estimate?

○ Yes

● No – Does not require a cost estimate

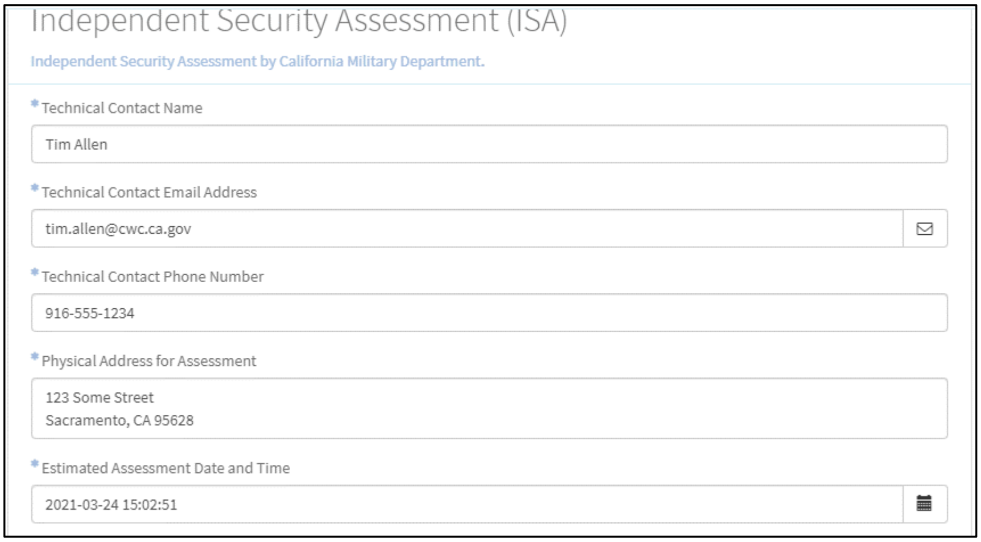
○ No – I have received a cost estimate

What is your approved budget amount?

*I understand that CDT will charge my department the applicable rates and/or pass-through charges for the services being requested.

□ Yes

10. Enter ISO or Entity Liaison Name, email address, and phone number. Enter the location of the ISA, to include any floor or suite numbers. Enter date of scheduled ISA, as provided on the notification letter.



Independent Security Assessment (ISA)

Independent Security Assessment by California Military Department.

*Technical Contact Name

Tim Allen

*Technical Contact Email Address

tim.allen@cwc.ca.gov

*Technical Contact Phone Number

916-555-1234

*Physical Address for Assessment

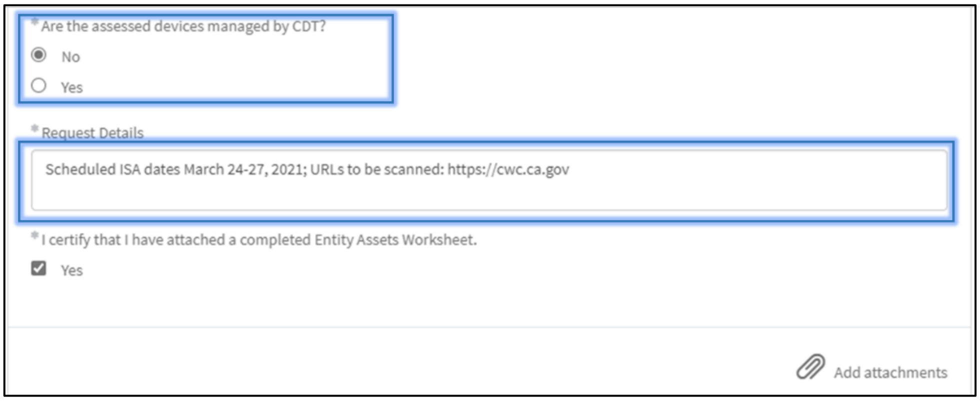
123 Some Street
Sacramento, CA 95628

*Estimated Assessment Date and Time

2021-03-24 15:02:51

11. Identify if assessed devices are managed by CDT. CDT Managed devices include, but are not limited to, the following: CDT hosted websites (shard host, WordPress, TMS, etc.); CDT managed firewall; CDT managed switch/router infrastructure devices; CDT hosted servers; CDT managed O365 email administered by CDT; CDT managed Anti-virus or Endpoint Protection configuration deployed on your hosts; CDT managed perimeter IDS/IPS configuration; CDT managed active directory. If you do not have CDT managed devices, follow step 10a below. If you do have CDT managed devices, follow step 10b. ***Note:* Failure to properly identify CDT managed devices will require a new Case to be opened in ServiceNow.**

    a. **Non-CDT managed devices:** If you do not have any services (webhosting, servers, firewall, etc.) managed by CDT, select "No". Using the "Add attachments" icon, add the completed Asset Count Worksheet. If more information is needed, add to Wish List to save or if complete, select "Order Now".



* Are the assessed devices managed by CDT?

● No

○ Yes

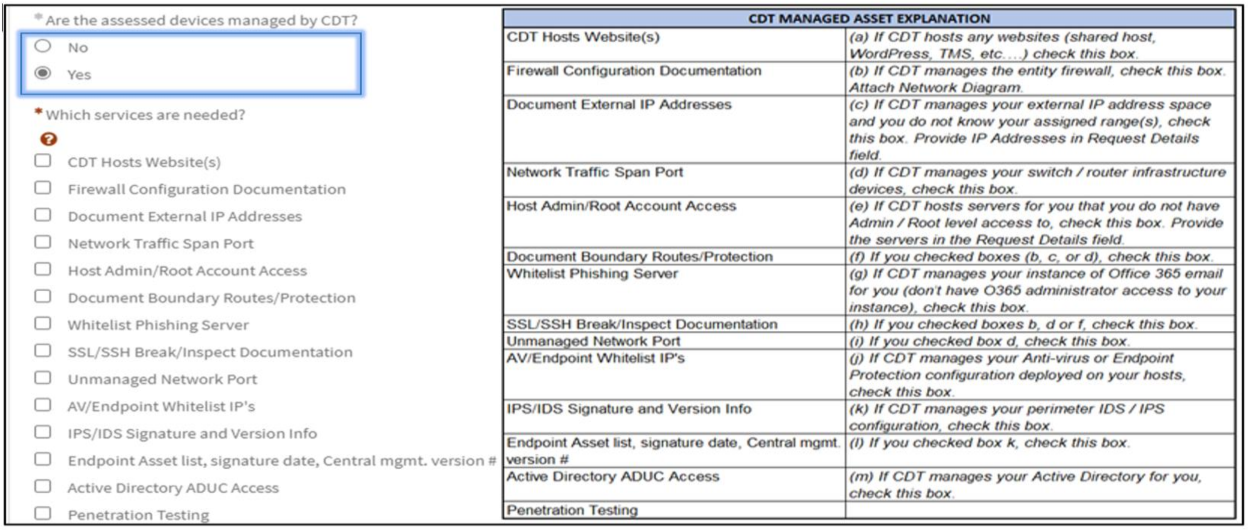
* Request Details

Scheduled ISA dates March 24-27, 2021; URLs to be scanned: https://cwc.ca.gov

* I certify that I have attached a completed Entity Assets Worksheet.

☑ Yes

    b. **CDT Managed Devices:** If you have any services managed by CDT, select "Yes". Follow the instructions in the "More Information" box to determine your CDT Managed Devices. **If CDT manages an entity's firewall, a separate Firewall/ACL request must be opened. Please reference your ISA Case number in the request along with the scheduled ISA dates. This will need to be opened after your ISA has been scheduled.** If more information is required, select "Add to Wish List" to save or if complete, select "Order Now".



* Are the assessed devices managed by CDT?

○ No

● Yes

* Which services are needed?

□ CDT Hosts Website(s)

□ Firewall Configuration Documentation

□ Document External IP Addresses

□ Network Traffic Span Port

□ Host Admin/Root Account Access

□ Document Boundary Routes/Protection

□ Whitelist Phishing Server

□ SSL/SSH Break/Inspect Documentation

□ Unmanaged Network Port

□ AV/Endpoint Whitelist IP's

□ IPS/IDS Signature and Version Info

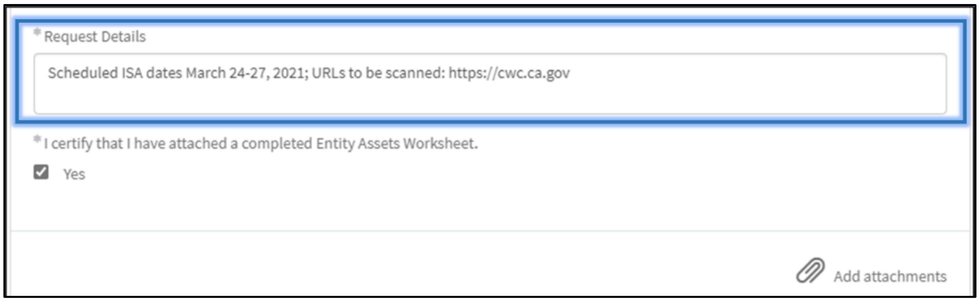
□ Endpoint Asset list, signature date, Central mgmt. version #

□ Active Directory ADUC Access

□ Penetration Testing

CDT MANAGED ASSET EXPLANATION	
CDT Hosts Website(s)	*(a) If CDT hosts any websites (shared host, WordPress, TMS, etc….) check this box.*
Firewall Configuration Documentation	*(b) If CDT manages the entity firewall, check this box. Attach Network Diagram.*
Document External IP Addresses	*(c) If CDT manages your external IP address space and you do not know your assigned range(s), check this box. Provide IP Addresses in Request Details field.*
Network Traffic Span Port	*(d) If CDT manages your switch / router infrastructure devices, check this box.*
Host Admin/Root Account Access	*(e) If CDT hosts servers for you that you do not have Admin / Root level access to, check this box. Provide the servers in the Request Details field.*
Document Boundary Routes/Protection	*(f) If you checked boxes (b, c, or d), check this box.*
Whitelist Phishing Server	*(g) If CDT manages your instance of Office 365 email for you (don't have O365 administrator access to your instance), check this box.*
SSL/SSH Break/Inspect Documentation	*(h) If you checked boxes b, d or f, check this box.*
Unmanaged Network Port	*(i) If you checked box d, check this box.*
AV/Endpoint Whitelist IP's	*(j) If CDT manages your Anti-virus or Endpoint Protection configuration deployed on your hosts, check this box.*
IPS/IDS Signature and Version Info	*(k) If CDT manages your perimeter IDS / IPS configuration, check this box.*
Endpoint Asset list, signature date, Central mgmt. version #	*(l) If you checked box k, check this box.*
Active Directory ADUC Access	*(m) If CDT manages your Active Directory for you, check this box.*
Penetration Testing	

12. Request Details: Enter scheduled ISA dates for ISA, the IPs or URLs of all CDT hosted assets (i.e., websites) to be scanned and any additional information here. Attach a completed copy of the Asset Count Worksheet to the request before completing the Order. For more information regarding this requirement, please contact your assigned CDT Account Lead.



* Request Details

Scheduled ISA dates March 24-27, 2021; URLs to be scanned: https://cwc.ca.gov

* I certify that I have attached a completed Entity Assets Worksheet.

☑ Yes

13. After the order is complete, OIS will provide the completed Initial Asset Count Worksheet and Case number to the CND Engagement Manager. The CND Engagement Manager will contact the entity to provide the Cost Estimate/Work Authorization (CE/WA). Once the CE/WA has been signed by the entity (ISO, CIO or other designee), email a copy to the CND Engagement Manager and attach a copy to the Case in ServiceNow.

Additional Information:

- As previously stated, the Initial Asset Count Worksheet and ServiceNow Case Number must be uploaded into ServiceNow to receive a Cost Estimate. For any clarification information regarding the Initial Asset Count Worksheet, please contact the CND Engagement Manager at info@cnd.ca.gov.

- **Do not add Data Call worksheets to ServiceNow**. Data Calls contain sensitive information about your network and should not be uploaded in ServiceNow.

- Once a Case has been submitted, you cannot edit any information submitted on the order form. Failure to identify CDT managed devices may require a new Case to be opened.

- After the entity has received their report CND will invoice CDT/OIS, OIS will close the Case.