CALIFORNIA MILITARY DEPARTMENT

CYBER NETWORK DEFENSE

INDEPENDENT SECURITY ASSESSMENT

PHASE II

ENTITY PREPAREDNESS GUIDE

Pre-Assessment Preparation
On-site Configuration Requirements
Assessment Requirements
Post-Assessment Delivery

Version 5 dated 5/20/2021
Previous editions are obsolete

Legal Notice, Disclaimer, and Licensing

Please note that much of this publication is based on prior professional experience and anecdotal evidence. Although the author and organization have made every reasonable attempt to achieve complete accuracy of the content in this guide, they assume no responsibility for errors or omissions. The practices contained here within are designed to facilitate a successful Independent Security Assessment (ISA) from the California Military Department. When guidance within the publication conflicts with your existing internal security protocols and practices, seek clarification with the Cyber Network Defense (CND) team engagement manager. Implement / retain these settings at your own risk. Your situation may not be exactly suited to the examples illustrated here as every entity's network is unique. If you have questions on how to proceed, please contact the CND Engagement Manager for assistance at 916-854-4CND (4263) or via email at info@cnd.ca.gov.

Any trademarks, service marks, product names or named features are assumed to be the property of their respective owners and are used only for reference. There is no implied endorsement of said products or services.

Table of Contents

Purpose of the Independent Security Assessment

Cybersecurity within the enterprise is a series of complex interactions in a constant state of change. The Independent Security Assessment (ISA) is designed to provide the assessed entity a third-party analysis of their as-deployed cybersecurity controls under measurement. The outcome of the assessment is designed to help validate program success and assist in identifying areas that require additional review. Entities that embrace the program and its findings benefit from the knowledge transfer it provides as well as make a profound statement as to their overall cyber maturity. The assessment criteria used within the ISA is under the control of the California Department of Technology (CDT), Office of Information Security (OIS). Participation within the assessment program is mandated in accordance with California State Code 11549.3.

Key Roles within this Guide

This guide identifies a series of tasks and requirements for entity success. These requirements are mapped to a series of roles. To effectively align each entity to the uniform requirements, use the below table (Table 1).

Table 1: Key Roles

Role	Description	Notes
Senior Cybersecurity Manager (SCM)	Responsible for daily entity cybersecurity operations management. Retains oversight of cybersecurity defense actions and change management within the organization. Typical role holders can include the CIO, AISO, and ISO. This individual will perform the role of entity assessment coordinator.	Do not delegate this role. Delegation of this role could place your assessment at-risk of lower performance.
Senior Network Administrator (NETADM)	Senior member of the Network Administration team with hands-on access to network infrastructure devices. NETADM has change management and configuration change approval.	Responsible to ensure all logical access controls requirements are met prior to ISA start.
Senior System Administrator (SYSADM)	Senior member(s) of the Systems Administration team with hands-on access to host configuration change and account creation/management authority.	If this role is divided between Windows and Linux teams, then assign the senior individual from the Windows / Linux teams to this role.
Service Desk Manager (SDM)	Manager with oversight to the call center, support desk, and other client initial points of technical assistance.	If SDM does not control phishing notice release, the individual responsible should be identified and included.
Entity Liaison (EL)	Primary on-site interface person between Risk Analysis/Penetration Test Teams and the entity. Except for extreme cases, one person should be assigned as the EL.	Individual should be technical and have change control notification. SCM can fill role in smaller entities.
CND Engagement Manager (CEM)	Serves as the single point of contact for all ISA aspects related to scheduling, pre-assessment coordination, pre/post assessment questions, artifact delivery, out briefing, and billing related matters.	Ensure you cc the CEM on all message traffic related to your ISA. This facilitates questions or issues are addressed rapidly.

Introduction to Preparing for the Independent Security Assessment (ISA)

The Preparedness Guide provides a series of preparatory requirements, recommended approaches, and suggested timelines to assist entities achieve the best outcome when undergoing an ISA. Your assessment will analyze a series of foundational cybersecurity technical controls, as designated by the OIS. Due to the constrained timeline for each ISA, an ill prepared entity can fail to achieve the program desired analytical outcomes and negatively impact overall ISA results. The entity is responsible for proper allocation of time and staff to ensure the successful participation during the scheduled assessment window.

> **Note: The ISA Criteria has adapted to conform with reduced contact procedures. The key to these reductions is the entity's successful pre-assessment preparation.**

Two Team Approach

The CND conducts the ISA using a two-team approach. The Risk Analysis (RA) team conducts tasks related to the defensive controls assessed (task sections 10-15). The Penetration Test (Pen Test) team conducts activities related to the offensive simulation operations portion of the assessment (task sections 16-17). These two teams operate independently of each other and conduct operations at different intervals (detailed later in this document). The combined team dispatched for your assessment will be between 2-6 members, depending on engagement size and number of days. The exact team size and team member make-up will be provided during your Pre-Assessment briefing.

Impacts to Ongoing Operations: The assessment will add additional network traffic and load to servers, workstations/laptops, and appliances on the assessed network segments. The CND is well versed in performing these activities with the least impact to the operational environment. As a matter of general operations, the CND will not perform actions known to create denial of service or significant degradation of services. If at any time, the Entity Liaison (EL) identifies a significant impact to ongoing operations, they should immediately report that to the RA Team lead. CND will reevaluate the offending activities and attempt to re-tune or shift operations to reduce/eliminate the issue.

Risk Analysis Team: The RA Team is responsible for assessing the tasks associated with enterprise defense processes. They are the entity's trusted assistance team. The entity will be sharing configuration information and credentials with the RA Team during the ISA process. Credentials, accesses, and configuration information provided to the RA Team is not shared with the Pen Test Team. The RA team also serves as the direct conduit between the EL and the CND's on-site staff. In the absence of the RA Team leader, please default questions directly to the CND Engagement Manager (CEM) unless otherwise directed in this guide.

The RA Team operations begin upon their initial arrival on the entity site. This will include a Team Introductions meeting with the identified assessment role holders. This is the time when all deliverables identified in Appendix G are due to the RA Team lead. During the meeting, the RA team lead will identify requirements and begin the scheduling of observed and physical tasks. It is absolutely critical to your success that all ISA role holders are in attendance. During the assessment, the RA team will conduct task 10.8, User Phishing Practical Exercise. This task is designed to measure the effectiveness of user awareness training. At no time will the RA team attempt to deploy malicious code to these targeted users. If the RA team successfully solicits credentials from the target users, they are not shared with the Pen Test Team.

Penetration Test Team: The Pen Test Team represents a group of simulated threat actors who have targeted the entity's network for possible network compromise and exploitation. The purpose of the engagement is to help the entity better understand live risk with the environment. Pen Test Team actions are often very noisy comparatively. This is due to the time constraint .vs cost tradeoff placed on the assessment. During a typical engagement, you will have very limited interaction with the Pen Test Team. The entity should not provide defensive configuration information to the Pen Test Team. If the entity member attempts to interact with a Pen Test Team member to share information that is intended for the RA Team, the entity member(s) will be stopped and redirected to the RA Team or CND CEM (as appropriate). There are three exceptions to this interaction between the entity and the Pen Test Team:

1. *Penetration Test Team Activity Detection:* During the engagement, when entity deployed cybersecurity detective tools detect signs of the penetration test activities, the EL is encouraged to:
   - Provide consolidated notifications of Pen Test Team events to assist the team in understanding the level of visibility of detections
   - Provide the ability for the entity to confirm observed activities are Pen Test Team activities. When reporting suspected suspicious activities, the EL is expected to provide the following information:
     a. Host(s) impacted
     b. Actions Observed
     c. Source of Actions (if known)
     d. Tool Detection Event Summary

2. *Significant Risk:* The Pen Test Team will initiate a *"Hard Pause"* if it detects a risk deemed so significant that delayed disclosure is likely to result in network compromise by a real-world threat actor. A hard pause is an immediate halt of all actions conducted by the Pen Test Team on the identified resource and requires immediate confidential reporting to the EL. The Pen Test Team will provide the EL information pertaining to the detected risk, impacted host(s), and recommended course of action to reduce the risk to the enterprise.

3. *Illegal Activity:* If the CND detects the potential presence of illegal activity (external threat actor compromise, insider threat activities, etc.) the ISA will initiate a *"Hard Sto*p". In a stop action, the Pen Test Team lead will work with the EL and their management team to perform the required initial reporting to Cal-CSIRS as well as facilitate any interim evidence preservation process for red team actions. Once declared, a Hard Stop will remain in effect until the CHP Cyber Crimes team releases the network for continued CND actions. This is done to prevent penetration test activities from damaging evidence. Depending on the length of the ISA and length of the stop action, this may result in the ISA being rescheduled to another available date in the ISA calendar.

Important Note: The ISA Team will never attempt in-person social engineering of your staff.

Penetration Test Segments

The Penetration Test portion of the ISA is divided into two testing segments:

External Segment: During this portion, the offensive operations team is simulating a threat actor commonly associated with activities such as ransomware and account theft. These activities are:

- Identified in ISA criteria tasks 16.1-16.9
- Performed off-site using CND operated infrastructure

- Actions begin on the first day of the Penetration Test External Phase (see Pre-Assessment Notification)
- Includes spear-phishing events (see Appendix E for rules of engagement)
    - May include CND controlled malware designed to create a foothold on the entity's hosts.

Internal Segment: During this portion, the offensive operations team is simulating an insider threat, in an assumed breach condition within the internal entity network. This includes providing the team one valid active directory account as identified in Appendix D. These types of actors engage in tactics designed to compromise networks, hosts, obtain sensitive information, and exfiltrate critical data. These actions are most closely associated with cybercrime and lower-level nation-state actors. These activities will commence upon arrival to the entity facility and connection of the Pen Test Teams assets to the network. They do not include further Pen Test Team spear-phishing actions. These activities are:

- Identified in ISA criteria tasks 17.1-17.6
- Performed on-site while direct connected to the entity network infrastructure
    - Entity is never authorized to disable, throttle, or interfere with the team connection. Failure to comply is a Rules of Engagement Violation and may result in invalidation of your ISA
    - Entity is authorized to address issues / concerns to the Pen Test Team lead this includes perceived degradation of service, bandwidth saturation, and host instability

Penetration Test Closeout Summary and Technical Exchange: Occurs on your last day of the internal Penetration Test. To determine the specific date and time that this briefing will be provided, please coordinate with CEM at least 20 days prior to start of the ISA.

This meeting can be conducted via Microsoft Teams or in person. If conducted in person and to ensure the maximum ability to knowledge transfer and demonstration, the conference room this meeting is provided in must:

- Have access to the same network segment assigned to the Pen Test Team
- Provide a projector or display panel that supports HDMI
- Offer adequate seating to accommodate the CND team members and entity invited participants
- Supports appropriate spacing requirements in accordance with CDPH / CDC / Cal-HR safety Guidelines

Differentiating Penetration Testing from Red Team Engagement Operations

The ISA includes a Network Penetration Test. This activity is dramatically different from a Red-Team Engagement. To better assist the entity's understanding of the differences and excepted actions in order to prevent a Rules of Engagement violation, the following summary is provided.

Intent of the ISA Penetration Test

- Provide a rapid assessment of the as-deployed technologies [#]
- Identify risks that could result in Host / Network / Data / Enterprise compromise before an external threat actor leverages for malicious advantage
- To provide insight as to the performance or security tools detection, alert effectiveness, and configuration
- Assist in prioritizing cybersecurity spending (personnel, equipment, and software)
- Support the efforts of the management team through validation of deployed security controls and asset protections
- Provides recommendations on remediations that will inhibit future threat actor success
- Provides technical team walk-thru of tool sets, techniques, designed to assist in the tuning of existing security infrastructure

What the Penetration Test is Not

- A Red-Team Event
  - Defined as: A full-scope, multi-layered attack simulation designed to stress security teams and defensive measures using real-life adversary tactics to avoid detection. This type of engagement assumes both teams will employ offensive measures to thwart and frustrate the other goals.
  - Typically, 5x longer in duration and cost
  - Assumes a limited scope and restricted pre-notification (excludes security team members) in order to measure the maturity of the defensive team
- Representative of the as-deployed cybersecurity technologies and Run-Books
  - [#] Inhibits some defender activities (disabling access, password resets, reimage of hosts)

Guide Purpose and Dissemination

This guide is designed to help the entity prepare for a successful ISA. It is critical that this document be disseminated internally to the responsible individuals holding the roles identified within the document and additional support staff, as appropriate.

The Entity Liaison (EL) is responsible to ensure the entity's efforts achieve the desired state of readiness prior to the assessment start date. Delays, missing documentation, or absent staff prevent the assessment team from rendering a complete assessment in the time frame allotted and may result in 'Non-compliance' findings. Please help the CND assist your organization gain the most benefit possible by ensuring full readiness.

It is the EL's responsibility to ensure this guide is provided to each assigned ISA Role holder as an attachment to your internal ISA Planning Meeting (typically within 10 days of receipt of scheduling emails). The EL should use the Pre-Assessment Section of this guide to assist their organization plan for and measure progress towards full ISA assessment readiness. Reoccurring meetings, increasing in interval as the start date nears will help the EL assess issues and resolve readiness challenges. A key benchmark for planning will be a sensing meeting with the collective role holders no less than 7 days prior to the Pre-Assessment briefing. This meeting should include an in-progress review of all tasks to ensure status is progressing appropriately and ensure individual role holder questions and concerns are identified so they may be address in the Pre-Assessment briefing.

Planning for Staff Impact

The CND recognizes staff time is valuable and limited. This guide is designed to provide insight in obtaining the highest state of readiness while lowering the impact on the staff to the minimum level possible. Staff impact depends upon the entity's level of technical expertise, current cybersecurity practices, access to funding, and existing documentation. To assist in minimizing impacts during the assessment, the following guidance should be adhered to:

- During the assessment window defer network changes (e.g., software upgrades, hardware replacement, GPO changes, etc.…).
- Lock network security changes to the environment no less than 15 days prior to the ISA window.
- Monitor and validate Key Role team members are onsite and/or available during the assessment window to provide troubleshooting assistance as required.
- The EL must be on-site and available to the team during each day of the ISA.

Preparing for ISA Success

The following sections were developed based on prior experience to assist entity preparation for their ISA. By using these lists and timelines, it will both reduce unexpected events and assist the SCM to ensure maximum preparedness. The provided timeline lists are broken down into the following event collections:

- Pre-Assessment Actions
- During Assessment Actions
- Post-Assessment Actions

Additionally, we have provided significant details for several activities in Appendix's A-I.

Post Assessment Activities and Report Delivery

Once the ISA team leaves the entity site your final reports and artifacts go through an extensive quality assurance process. This process takes between 4-6 weeks. The on-site ISA Team is unable to provide these status updates during the QA period. For the assistance in determining delivery status or to answer any questions regarding your ISA, please email us at email info@cnd.ca.gov.

Once the ISA out brief is scheduled the EL and ISO will receive an email with a download link approximately 24 hours prior to the briefing. This link provides access to an encrypted executable file containing a copy of the report and its artifacts. You will receive the complete decryption password during your out brief. If the EL and the ISO listed on the POC tab in the ISA Data Call has changed since the ISA Team have left entity site, it is Entity responsibility to provide updated contact information to CND at info@cnd.ca.gov. In accordance with California State Code 11549.3, a copy of the report is forwarded to CDT ISO and OES Cal-CSIC.

Pre-Assessment Section

The pre-assessment portion details all tasks that should occur prior to the ISA start date. Day notations are recommendations. It is the entity's responsibility to ensure proper assignment and execution of all actions to ensure the necessary outcomes are completed prior to the required Section (Pre-Assessment, Assessment). However, CND will review your status of the tasks completed.

Task Role Cross-Reference

- Organizational Chief Information Security Officer or ISO if none assigned (CIO)
- Senior Cybersecurity Manager (SCM)
- Senior Network Administrator (NETADM)
- Senior System Administrator (SYSADM)
- Service Desk Manager (SDM)
- Entity Liaison (EL)

Task	Roles	Task Detail	Days Prior to ISA Start	Complete
1	CIO	Designate SCM and EL. Provide contact information on Tab 2 of the Data Call Worksheet	90+	
2	SCM	Self-Identify to CND Engagement Manager via email at info@cnd.ca.gov	90+	
3	SCM	Distribute Preparedness Guide to individuals who are assigned roles within the assessment / guide	90+	
4	SCM/ SysADM/ NetADM	Review ISA Criteria and understand what will be assessed. Write down any questions in preparation for the Pre-Assessment Briefing. Notify appropriate parties to be prepared to present proof to ISA team when requested and verify status of readiness.	75+	
5	NetADM	Identify externally accessible public IP space and resources on Tab 4 of the Data Call Worksheet (see Appendix A)	70+	
6	NetADM	Identify internally used IP space and resources. Complete Tab 5 of the Data Call Worksheet (see Appendix A)	70+	
7	SysADM	Identify website owners (see Appendix B) on Tab 6 of the Data Call Worksheet; ensure all Hosted entity websites are listed.		
8	SCM	Identify nominated phishing participants. Complete Tab 7 of Data Call Worksheet (see Appendix E)	70+	
9	SCM	Submit Data Call Worksheet to CND Engagement Manager (info@cnd.ca.gov)	70+	
10	SCM	Identify sensitive data contents that would require entity's immediate notification if detected by CND externally (e.g., SSNs, account numbers, key words, technologies, etc.). Disclose at Pre-Assessment Briefing	70+	
11	SCM	A. Attend ISA Pre-Assessment Briefing and ensure all personnel assigned Key Roles attend. B. Provide an update on the status of all tasks on the Pre-Assessment Task List to the CEM C. Track remaining tasks and questions D. Identify critical concern data exposures E. Ensure all organizational requirements are completed prior to ISA start date	70+	

Task	Roles	Task Detail	Days Prior to ISA Start	Complete
12	Sys ADM	Notify 3rd party hosts for externally hosted web applications/sites and document approval	45+	
13	SCM	CDT Managed Firewall Services (FaaS): CDT managed Firewalls require a separate ServiceNow Case. There are two tasks that will require two separate ServiceNow Case numbers. A.) Mirrored Span Port for traffic capture; B.) Firewall Configuration A. Coordinate with CND Engagement Manager to ensure the correct span port is opened prior to request. B. Coordinate with CND Engagement Manager for requirements.	45+	
14	SCM/ NetADM	Identify a workspace for the CND team for the entire assessment period. The teams will be co-located. Workspace must meet the following requirements: • Accommodate team personnel identified in Pre-Assessment Briefing • Inform NetAdmin of the reserved room number so they can configure a port as appropriate for the Network Access Switch as listed in Appendix C • Workspace should afford privacy from common space (e.g., Conference Room) with a lockable door	45+	
15	SCM	Coordinate RA Team Introductions with CND Engagement Manager and invite Entity key roles (Infosec Management. System Admin, Network Admin, EL). Include CND Engagement Manager in the meeting invite. This can either be in person or via Microsoft Teams.	20+	
16	SCM/Sys ADM	Coordinate with the Pen Test Team lead on the first day of the Internal Penetration Test at 10:00 AM for the date/time of the Penetration Test Closeout Summary and Technical Exchange and AD account. (See Appendix D for Account Creation). This can either be in person or via Microsoft Teams.	20+	
17	NetADM	A. Identify any network blocking technology (ACL, Firewall rules, IPS, etc.) between management subnet and all hosts on network B. Implement measures to enable RA Team scanners access to **all** Entity Systems.	20+	
18	Sys ADM	A. Identify any host-based blocking technology (HIPS, AV, etc.) between management subnet and all hosts on network **(RA Team ports only)** B. Coordinate with NETADM to implement measures to mitigate via Group Membership, VLAN, or other security methods	20+	
19	Sys ADM	Ensure internal host services are available for Vulnerability scanning as identified in Appendix D	17+	
20	NetADM	Configure switch for the provided ISA space and prepare IP address requirements as listed in Appendix C.	10+	
21	Sys ADM	A. Identify 10 hosts by host name and IP address (3 workstations, 3 laptops, 3 Application Servers, and 1 Domain Controller) for system hardening assessment	10+	

Task	Roles	Task Detail	Days Prior to ISA Start	Complete
		B. Provide list of target hosts to SCM		
22	SCM	Validate all required key roles will be present for ISA	10+	
23	NetADM	Provide network interconnection diagram to SCM for RA Team documentation	8+	
24	Sys ADM	Prepare accounts for RA Team in accordance with Appendix D.	8+	
25	Sys ADM	Whitelist CND provider IP address for phishing campaign (see Appendix F)	7+	
26	SCM	Prepare Entity appropriate Unescorted Building Access badge requirements (required for delivery to Team Leads on initial day on facility) as discussed in Pre-Assessment Briefing	7+	
27	Sys ADM	Disable and verify Sleep/Power Saver functions to disabled to prevent host unavailability during off hours (Mandatory)	3+	
28	NetADM	Establish span port to mirror egress/ingress network traffic between inside of firewall and network core switch in preparation for the network traffic capture	3+	
29	NetADM	Deploy/test access switch in designated workspace for ISA Team usage (previously configured in Task 23)	1	

Assessment Section

This section details all the tasks that occur during the ISA Assessment phase.

Task	Roles	Task Detail
1	EL	During External Pen Test immediately notify CND if you notice anything anomalous events (e.g., System anomalies, rogue device detection, phishing detection) on your network during the entire ISA. Notifications of detections are time sensitive for scoring purposes prior to taking any action. If RA Team is not on site, contact CND Engagement manager via phone.
2	SCM	Deliver any updates/materials not previously delivered to RA Team during RA Team Introductions (see Appendix G)
3	SCM/EL	Ensure RA Team has appropriate contact info, workspace access and network access
4	EL	Notify RA Team or CND Engagement Manager if RA Team is not on site of any Phishing Campaigns detected prior to entity response/action. **Note: See Appendix E for Complete Rules of Engagement.**
5	SysADM	Coordinate with the Pentest lead to randomly select the insider threat account for Internal Pen Test team use not later than 1PM on this first internal Pen Test day. (See Appendix D)
5	EL	Notify RA Team of unusual activities detected by network admin/system admin to determine if they were initiated by Pen Test Team or other activities
6	NetADM	Facilitate assistance to have Firewall Administrator generate required configuration files for delivery to RA Team
7	SCM/EL	Coordinate with Pen Test Team in event of hard pause

Post-Assessment Section

This section entails the tasks that occur during the post ISA Assessment phase.

Task	Roles	Task Detail
1	EL	Coordinate deactivation of badge access, network access/accounts, etc. to fully deprovision CND access
2	SCM	Receive notification of Password Reset for compromised accounts
3	CEM	Notify the entity the final report is ready for delivery and schedule delivery date; send out brief meeting Invite to Entity Key Roles and individuals SCM identifies as being required for out briefing, AIO, CIO, etc.
4	CEM	Ensure secure electronic delivery of final brief products; provide 1st half of secure decryption password 1-3 days prior to out brief
5	SCM	Schedule conference room and notify entity key roles and appropriate management team members of location
6	CEM	Initiate Out Brief. Facilitates meeting as required
7	SCM	Following the Out Brief, validate all files are complete and viewable. Request replacements for damaged files (as applicable)
8	SCM	Review results with larger IT teams. Determine courses of action for remediation. Determine timelines
9	SCM	Prepare Plans of Action and Milestones (POA&M) for submission to CDT
10	SCM	Submit POA&M to CDT via secure FTP server (within 30 days)
11	SCM	Update POA&M as required

Appendix A - Data Call Worksheet Scoping (Tabs 4 & 5)

Tabs 4 & 5 contain some of the most important information the entity provides in the Data Call Worksheet. Providing accurate data will reduce entity time and effort while improving the quality of the ISA results.

Purpose: To ensure your assessment provides the highest degree of risk insight, the entity MUST accurately identify all entity information technology (referred to as assets). Proper identification of all IP ranges is vital to a successful ISA. To support the ISA activities by both teams and both segments (External and Internal), the Data Call Worksheet provides two Tabs, External and Internal.

***Note:* Failure to accurately identify all IT assets / IP ranges may result in non-compliance findings.**

Scoping Considerations: Generally, the entity will consider all computer hosts (Servers, Workstations, Desktops, Laptops, and Appliances with an IP address) that the entity has privileged/administrative access, that reside within the entity allocated IP address space or on a 3rd party hosted networks as In-scope. Regardless of scoping, all IP ranges MUST be identified.

- Examples of In-scope hosts:
  - Windows, Unix, Linux, BSD, Apple hosts (workstations, notebooks, laptops, servers, virtual servers, bare metal host, network appliances, thin clients, IoT devices, etc.) that the entity has root or administrator level log-on rights
  - Third-party hosts residing in the Entity IP Address space in which the entity is responsible for the validation of the hosts' security configuration
  - Microsoft Azure / Amazon / AWS / Salesforce / etc. cloud hosted hosts (e.g., domain controllers, file and application servers, web servers)
  - 3rd Party web/application servers hosted in non-State of California managed data centers

- Examples of assets potentially eligible for an out-of-scope exception request
  - A host owned by another agency (not covered under this assessment) that the assessed entity(s) does not have configuration management or privileged rights access.
  - A host that provides life-preserving services, which if rendered off-line for greater than 10 minutes, could result in loss of life, catastrophic financial damage to citizens, or significant damage to property.
    - A detailed justification must be submitted for each item listed
    - An evaluation to determine acceptance will be conducted at the Pre-Assessment brief.
  - A host designated critical IT asset that is suffering from stability issues; if unexpected reboots were to occur could result in an unrecoverable condition and loss of data (unstable, unrecoverable high-risk hosts).
  - 3rd Party provided cybersecurity sensors / collectors (e.g., sensors monitored directly by CDT SOC / Cal-CSIC)

- Examples of off-premises services: For example, Entity contracts with BMC to use their Information Technology Service Management system (aka ServiceNow). Entity is not privy to the specifics of the architecture nor does it manage the application at the server level.
  - Here are 4 scenarios to help address this complex example:
    - If state funds are used to procure a 3rd party service, then technically it is in scope. In many cases, these are web applications that should be listed in Tab 6 (Public Facing Websites) and required 3rd party notification. Refer to DGS requirements for contracts, requiring a clause for security validation testing (e.g., ISA). If the vendor refuses assessment, please notify CND so we can notify the CISO office of the non-compliant vendor.
    - Cloud Provider Business Services for Email and Document Management (e.g., M365 / Google Mail Services / Adobe Cloud Document Management). These services are required to be

hosted in a FedRamp Government Cloud certified data center using an approved FedRamp Government template.
    - Azure / AWS hosted services (e.g., SQL Server configured by the entity) would be considered in-scope. The entity's ability to adjust / modify the configuration to potentially setting less than the FedRamp Government Moderate level require the asset to be assessed.
    - 3rd Party Applications certified by Independent Assessment. Some vendors require their hosted applications to be penetration tested. If the application in question undergoes 3rd party Pentest, obtain proof of testing occurrence within the past 24 months from date of assessment and include that certification with your request for out-of-scope.

- Requesting an Out-of-Scope exception for a host is an anomaly event; a typical assessment will not have any approved Out-of-Scope assets. If you believe you have a valid requirement for an Out-of-Scope host, list the asset in the Out-of-Scope list and prepare documentation to support the out-of-scope request. To reduce complexity, address these issues prior to the Pre-Assessment brief with the CND Engagement Manager. In cases where the asset is requested to meet the out-of-scope classification, enter that asset in the Out-of-Scope portion of Tab 4 and 5 and submit the justification documentation with your Data Call Worksheet.

**Please note: As the entity's option your Data Call Worksheet may be submitted via encrypted email to CND Engagement Manager.

- Must be coordinated in advance
- Do not enforce Digital Rights Access Restrictions that prevent the opening or viewing of the document. Multiple team members are required to access the content. Failure to follow this requirement will result in required document resubmission with controls removed.

IP Ranges: IP ranges for Tab 4 and Tab 5 must be listed in address blocks no larger than a CIDR notated Class "C" (/24) in size. If only a single IP address is in use, either list it separately or as a x.x.x.x/32 address**. The Entity should NOT list a CIDR Block or IP address range larger in a /23 (512 IP's) as a single entry**. Entities unable to provide fine-grain detail on larger IP address blocks will require intrusive IP Scanning and may incur additional days of service at additional cost to fulfill the ISA requirements. If intrusive or out of hours scans are required, an adjustment to your cost estimate will be required.

Tab 4 – External Scoping

Steps:

1. Identify all IP addresses externally exposed to the internet. Sources include:

- Advertised IPs by CDT under the entity's control
- Hosted Entity IP ranges if you are a Host.
- External Router Advertisements
- Firewalls
- Cloud Assigned IP hosts (specific IP's as CIDR Blocks may contain multiple tenant assets)

2. For assets hosted on non-entity-controlled networks, you are required to determine the manner and method for notification and ensure it is performed with a minimum of 30 days prior notice. For assets hosted at CDT, this is performed using the ServiceNow ticketing system when you opened your ISA ServiceNow Case Number. Here are two scenarios to help clarify the requirement:

- *CDT Hosted Services (e.g., website running in the CDT data center on a shared WordPress server), are considered 3rd party. This is a shared resource using CDT data Center managed and* protected

IP address space. This asset should appear on Tab 4 and on the existing ISA ServiceNow case number *under CDT Managed Assets*.
    - *If listed in both locations,* no further action is required for this asset
    - *If not initially listed, then update the TAB and ServiceNow Case number to reflect the asset(s) within the CDT Managed Assets section*
- Tenant Managed Service (TMS) hosts within the CDT Data Centers are hosts under direct administrative control of the entity.
    - If individual hosts assigned IP is contained within an already provided contiguous IP address on Tab 4 (e.g., reachable via existing VPN tunnel from the entity network) and not directly Internet accessible, those assets should be listed on Tab 5 (Internal Scoping).
    - If directly reachable on the internet via a valid, routable Ip address, then the asset should be listed on TAB 4
    - If CDT manages the Firewall directly between the host(s) and your VPN tunnel, no CDT notification is required for these hosts.
    - If the IP's used by these hosts are CDT Data Center controlled IP addresses, then these host(s) must be listed on the existing ISA ServiceNow case number *under CDT Managed Assets*.
- Carrier provided infrastructure (e.g., Edge routers, cable modems, and other layer 3 devices) that are assigned an internet routable IP address.
    - External IP will be listed on TAB 4 and the entity must be notified that the assets will be scanned for vulnerability.
    - Internally assigned entity address will be listed on TAB 5
- Virtual Hosts and services deployed within a cloud service provider IP range, either entity or deployed as part of a 3rd party provided service must be listed on TAB 4 and the provider notified.

*Note: When in doubt, please contact the CEM for guidance. Failure to declare assets may adversely impact your ISA.

Tab 5 – Internal Scoping

Steps:

1. Identify all IP addresses utilized on the internal, VPN, and hosted networks that are not externally accessible. Sources include:

- IPs assigned by CDT, Microsoft Azure, and other cloud providers, which are only accessible from inside the entity network and under entity control. This includes: Server Ranges (On-Prem and Cloud); IT Team Workstations; User Workstations/Laptops, Peripheral Devises (if unique Subnets), and Other.
- Hosted Entity IP ranges if you are a Host.
- Internal router advertisements
- Firewalls
- DHCP Scopes
- VPN Tunnels
- See above for additional scenarios

2. For assets hosted on non-entity-controlled networks, ensure the IP owner is notified of your ISA in accordance with their notification procedures.

3. For IP addresses hosted internally for assets not managed by the entity (e.g., another agency not under assessment, leased commercial hosts which the entity has provided a Pentest summary report completed in the past 12 months) the entity may place those IP addresses in the out-of-scope Justification block of Tab 5.

CND recognizes many entities may have concerns related to the release of internal network architecture documentation and IP address spaces. It is important to understand why this data is required in advance of the assessment period.

- CND RA/Pen Test Team must evaluate the provided data to ensure appropriate scoping is declared (range, CIDR, description). The restriction of data-call information for use only onsite is not authorized and not supportable.
- Any requested Out-of-Scope hosts must be declared and evaluated for approval prior to the ISA. Often concerns can be addressed, eliminating the request so long as these issues are discussed prior to the assessment start date.
- The ISA is a time-based event. To ensure the entity can receive a valid assessment, the IP space and asset counts must be reviewed prior to the Pre-Assessment Briefing to ensure adequate time is provided.
- Access to your provided Data Call IP address ranges are handled by personnel with a validated US Government Security background investigation of US Secret or higher and a confirmed Need-to-Know. This data is solely used to conduct the ISA. CND treats this data with the sensitivity required to protect the data while under its control.

Scoping Example Entries:

Section 1 - External Assets		
*** - Ranges no greater than 1,024 hosts each; List 1 line per Class C (/24) where hosts reside*		
## - Must specify only the specific IP's of hosts under the entities control		
Entity External IP Ranges In-Scope		
IP / CIDR **	**Purpose**	
23.17.45.0/24	DMZ-Webservers	
23.17.49.0/24	DMZ - External DNS, SQL Servers	
131.110.118.33/27	AWS Hosted Application	
23.20.15.17/28	AWS Hosted-Snap X Application	
Entity External IP Ranges - Out of Scope		
IP / CIDR ##	Purpose	**Justification**
67.111.30.9-11	AT&T Managed Infrastructure	**Justifcaiton Statement Here**

Section 2 - Internal Assets	
*** - Ranges no greater than 1,024 hosts each*	
## - Must specify only the specific IP's of hosts under the entities control	
Entity Internal IP Ranges In-Scope	
IP / CIDR **	**Purpose/Description**
Server Ranges (On Prem, cloud)	
10.0.1.0/24	HQs Servers
10.0.10.0/24	LA Grover Street Servers
10.0.11.0/24	Cloud Servers
IT Team Workstations:	
10.0.2.0/32	IT Team Work Stations
User Workstations / Laptops:	
10.0.5.0/24	HQ workstations/laptops
10.0.6.0/24	HQ workstations/laptops
10.0.7.0/24	LA Grover Street workstations/laptops
10.0.8.0/24	LA Grover Street workstations/laptops
Peripherals Devices [if unique Subnets):	
10.0.3.0/24	HQS Rourters, Swtichers and firewall range
10.0.4.0/24	LA Grover Street Routers, Switchers and firewall range
10.0.13.0/24	HQS VOIP
10.0.14.0/24	LA Grover Street VOIP
Entity Internal IP Ranges - Out of Scope	
IP / CIDR ##	Purpose / **Justification**
10.0.1.110	IRS Death Ragister Gateway Server / **Justificaiton Statement Here**

Appendix B - Public Facing Websites (Tab 6)

Entities may have multiple internet-facing websites. Due to the time-based nature of the assessment, a best effort to assess up to 5 publicly accessible web sites will be considered in-scope for the Assessment. The Pen Test Team may determine additional sites will be targeted for limited penetration testing on an ad-hoc basis.

Purpose: To assist entities prioritize the highest value internet facing web properties, the following criteria should be considered when completing Tab 6 Public Facing Websites:

- Sensitivity of the information processed
- Likelihood of loss of life, property, or financial damage should the host / data processed be compromised
- Age and mitigative measures applied to the host
- The criticality of the host to providing core-services to the entity's constituency

Steps:

1. List the full URL for each publicly accessible web asset on Tab 6 (e.g., https://www.acme.ca.gov). If you are not sure how to proceed in this area, please contact the CEM for assistance.

- Subsites within a declared web host address (e.g. www.acme.ca.gov/research and www.acme.ca.gov/forms are already covered within the www.acme.ca.gov declaration UNLESS there is link on the base URL site to these subsites.

2. Order the web sites on TAB 6 using the following guidelines:

- Entry 1 must ALWAYS be the entity's primary public web site as this site is mandated for assessment. The primary web site is the web resource that includes the entity primary namespace within its address (e.g., https://www.acme.ca.gov) and is the commonly referred to resource for public information.
- If you have a Hosted Entity/Entities place the public web site as entry #2 and so on. For example your entity website is www.acme.ca.gov and your hosted entity websites are www.anvil.ca.gov and www.tnt.ca.gov, you need to list both hosted entity websites as priority 2 and 3. See example below. Reorder remaining sites based on a risk / priority rating.
- Do not list sites that are:
  - Not accessible from the public Internet
  - Only present a single page for logon only (exception: Any Remote Access Solution)
- Optional: If the entity desires a test of a website protected by password, coordinate with the CEM for additional guidance.

3. If the site is hosted in a Data Center not under the direct control of the entity (CDT, Amazon, etc.) then the entity must follow the host's established Web Pentest Notification Process. Contact hosting provider for additional information. If the host refuses to allow the site to be analyzed, please notify CDT OIS of the non-compliant host so efforts can be made to move your site to a location that meets state compliance standards. **If the entity lists a site for assessment without obtaining approval, the resulting penalties or costs associated with the event by the 3rd party host would be the sole responsibility of the entity.**

4. If the entity has significant concerns about a specific web application / site, please address those directly with the CND Engagement Manager.

NOTE: **If you save your web server logs on the same drive as your operating system, there is a chance that repeated analysis could fill the logs and cause your OS drive to run out of space. This is a risky configuration and should be resolved prior to the ISA to help avoid potential outages**.

Example Submission:

Priority	Entity Website URLs
1	https://www.acme.ca.gov
2	https://support.acme.ca.gov
3	https://owa.acme.ca.gov
4	https://acme.wp.com
5	

Appendix C – Network Connectivity Requirements

Deploy a switch with 8 dedicated 1GB copper ports in the provided ISA space. Switch uplink port must support 1GB access to the core switch. The deployed switch must be configured to comply with the following minimum requirements:

- *Required Port/Switch Configuration*
  - Disable ALL Port Security
  - Allow for multiple IP assignments on each port for connected Virtual hosts
  - Successfully test for access no less than 24 hours prior to the first day of assessment
  - Identify any questions related to connections to CND no less than 7 days prior to ISA start date
  - Mark the first 4 ports **RA Team** and the last 4 ports **Pen Test Team**

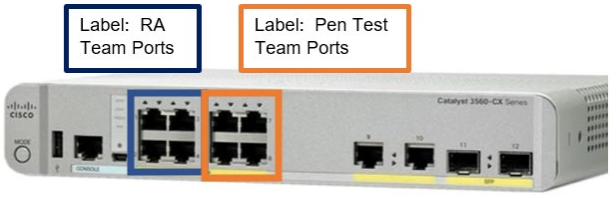


Figure 1: Example Labeling of Ports on Provided Switch

- RA team Port Configuration
  - Within the VLAN (Mandatory) that has unrestricted access to ALL hosts on the network (on-premise and cloud)
    - If this requires more than one VLAN, than this must be coordinated in advance and with hosts and associated credentials separated by IP
  - No ACL restrictions
- Pen Test team Port Configuration
  - Located in the entity's highest user density VLAN (your busiest user VLAN)
    - If the entity is still in a Work-from-Home environment, the VLAN provided must provide access to the VLAN that contains the Remote Access solutions internal IP address range
    - Note: *Due to **Work-from-Home** activities, if less than 100 users are working at the facility where the Pen Test Team is conducting activities, there must be a minimum of 25% of the work force working on site during the entire assessment period.*
  - Address issues or concerns VLAN placement or IP issuance during Pre-Assessment Briefing

Provide IP address requirements for ISA Team as listed below:

- RA Team
  - 8 static IP addresses; *Must* be Whitelisted in your Endpoint Protection and IDS/IPS technology solutions
  - Provide IPs during Team Introductions
- Pen Test Team
  - 9 DHCP IP addresses; Not required to be whitelisted

ISA Team Internet Access:

The ISA Team requires internet access while operating on your facility to perform tasks, update scoring, and monitor email. The entity may provide this in any number of methods that include but are not limited to:

- Via LAN connected access (e.g., Proxy authorization or bypass as appropriate)
- Via Guest Wireless access

Appendix D – Preparing Credentials

Risk Analysis Team Credentials: A significant portion of time will be spent during your ISA by the RA Team analyzing the maturity of the entity's vulnerability management program. This appendix specifies the mandatory requirements the entity must be prepared to meet. This appendix attempts to identify a broad range of potential scenarios that may apply to your environment. It is the responsibility of the entity CIO to ensure the required assessment conditions are communicated to their team and met no later than 7 calendar days prior to the start of the ISA and remain in place until the assessment is complete.

Vulnerability scanning will be conducted during the assessment. Ensure the following internal host services are available for Vulnerability scanning (SSH may have to be enabled for scanning purposes on Linux and mac systems):

- Windows Hosts
  - TCP/UDP ports 139,445 on modern hosts (Windows 10/Server 2012 and newer)
  - TCP/UDP ports 135,137 on legacy hosts (Windows 7/Server 2008 and older)
  - Windows Management Instruction (WMI) service enabled, see vendor guidance
  - Remote Registry Service must be enabled
- Non-windows hosts
  - tcp/22
- If modifying how these services are exposed to the network, ensure those modifications are only presented to the subnet the RA Team operates from
  - Unless otherwise restricted, these services are typically available as part of normal host management operations.

These scans will require credentials that meet the following standards:

- The provided credentials must have full access to all compute hosts:
  - Configurations
  - Registry (as applicable)
  - Services configurations
  - Logical device storage
- Credentials that meet this standard are typically categorized as:
  - Local Administrator for non-domain joined (stand-alone) Linux or Windows hosts
  - Domain Administrator in typical windows environments where role-based credentials do not segregate access by host function, type, or location
  - Device/Location/Function Specific Administrator Roles for entity's that have segregated access by host function, type, or location
    - In situations where credentials are segregated by host function, type, or location, credentials must be supplied that:
      - Map the specific host by resolvable host name and IP address to the unique credential set
      - Group like credentials sets / hosts into a single tab of a spreadsheet with the column headings of:
        - Host IP, Host Name, Username, Password
      - Present the spreadsheet in electronic form (via USB transfer or encrypted email) to the RA Team lead at the on-site kick-off meeting
- Depending on the entity environment, the following number and naming convention of require credentials are:
  - Windows Non-segregated environments:
    - CND_1 (Domain Admin or Equivalent Privileged role, no MFA enforcement)
    - CND_2 (Domain Admin or Equivalent Privileged role, no MFA enforcement)
    - CND_3 (Standard User Privileged role, no MFA enforcement)
  - Windows Segregated environments:

        - Two accounts named using the naming convention of CND_A..Z (Domain Admin or Equivalent Privileged role, no MFA enforcement) for each segregated environment
        - CND_3 (Standard User Privileged role, no MFA enforcement)
    - Non-windows Hosts / Stand-Alone Environments:
        - CND_Zn for each segregated host set where the credentials work
- Credentials must be static for the entire assessment period and may not be managed by 3rd party tools such as Privileged Access Management (PAM) or similar technologies
- Credentials must be configured during the assessment period to not require multi-factor authentication
- Credentials and the associated IPs issued to the RA Team must be white listed in all Security devices (e.g., Firewalls, Endpoint Protection, IPS/IDS, and other preventative measures)
- Credentials and the associated IPs issued to the RA Team must have uninhibited access through all entity utilized infrastructure devices, including but not limited to routed segments, switched environments, Software Defined Networks (SDNs), cloud networks, and Access Control Lists (ACLs) for the required ports identified by host type within this document
- Credentials must be access validated by the entity prior to the assessment
    - Consider cloning known, successful existing roles used for this function, renaming as identified, and positioned in the appropriate Organizational Unit (OU) as the original account (see PAM caveats).
    - Ensure once the new account(s) password is set, to uncheck the User Must reset password at login option
    - Should significant credential troubleshooting requirements occur during the assessment period that inhibit the timely analysis of the required hosts, this could impact the entity's ISA acceptance, triggering reassessment and rebilling.
        - Unaccepted ISA's are reported to the Legislature during the quarterly update and including a summary of conditions that led to the non-compliance.

Penetration Test Team: During the internal phase of the Pen Test, the team will be simulating the potential activities of an unknown Insider Threat within the entity environment. This portion of the assessment is conducted to help identify unrecognized risk with the entity environment. This includes the assessment beginning with valid network and active directory access. Doing so, streamlines operations and provides a more thorough account / permissions liability analysis.

Internal Pentest Only: As part of the initial Pen Test lead meeting, held at 10:00 AM on the first day of the internal Pen Test, the selection of the cloned user account will be accomplished. This activity will occur with the support of a member of the entity AD team (in person or via teams). The procedure for this activity is:

- Using AD Users and Computers, the AD team member will display the Organizational Unit(s) that contain typical users within their enterprise
    - In shared AD structures, users will be filtered to display only the assessed entity(s) users
- The Pen Test lead will randomly select and evaluate 3 active user accounts as the baseline to represent the insider threats access
- The Pen Test lead will review each randomly selected account access rights and document them for comparison purposes and will select one of the 3 documented accounts to represent the insider threat's access within the environment
- The Entity AD Team member will clone the selected account, change the logon to "CndPT" and reset the password, providing the credentials to the Pen Test lead
- The new CndPT account will not be disabled, inhibited, have its access altered, or otherwise changed by the entity once cloned
- Access to the provided account will be identified in the report pre-amble as a requirement of the assessment and its acquisition not counted against the entity for scoring purposes

Appendix E - Rules of Engagement, Phishing Events

Purpose: Phishing is the primary real-world method most threat actors achieve their initial foothold on networks. As a result, the ISA approaches this area in two different ways. It is important the entity clearly understands their expected actions under both approaches to ensure successful measurement. Entities cannot perform their own phishing exercise and provide the results to the CND. For the purposes of the ISA the test must be completely blind to the organization. While some entities perform internal phishing exercises, CND requires any exercises normally conducted by the entity to be suspended during the assessment period.

During the assessment two distinct types of phishing will occur. To ensure CND can effectively evaluate the phish-ability of the entity, some modifications will be required to be made to your phishing response procedures. These modifications are outlined below.

- Prior to Assessment Period
  - Execute the Whitelisting guidance provided (Appendix F)
  - If the entity has multiple physical / virtual security measures that inhibit message delivery, make comparable adjustments to those devices
- During Assessment Period
  - Receipt / previewing of phishing messages has no impact on the entity's ISA scoring
  - Once the campaign(s) are detected, the EL will immediately notify the on-site RA Team
    - Ensure EL has the RA Team lead cell phone number
    - EL will provide a hard copy of the email for review / determination if CND activity
    - Entity pauses any defensive actions regarding the email until determination is made
    - If the entity is unable to get a response from on-site RA Team lead within 10 minutes, call CEM at (916)854-4263. This individual's desktop phone rolls to their cell phone.
- Delayed Response Handling Procedure: If a response is not received using this method within 15 minutes of calling the CEM, to protect the enterprise, the EL will authorize:
  - Removal of the suspect message from the user(s) inbox
  - Bundle a screenshot the email, summarize the efforts for contact / verification and document the actions taken to attempt verification; email this to the CEM at info@cnd.ca.gov immediately.

Risk Analysis Team Nominated Phishing Event/Tasks: RA Team phishing exercise is designed to measure the effectiveness of user training with regards to the identification of a phishing attacks using modern phishing methods. The RA Team phishing examines the metrics associated with the number of user(s) that perform the following actions related to the message:

- Clicks on the provided link within the email
- Number of user surrendered credentials (if applicable)

For the purposes of this event, this is an information collection activity only. RA Team events *NEVER* include malicious attachments or other payloads.

Tasks listed below must be accomplished prior to ISA:

- The entity must provide a minimum of 100 users (up to 200 users may be submitted at the entities request) on Tab 7 - Phishing of the Data Call Worksheet. If the entity has less than 100 employees total, submit all employees.
- Submission must include the following data in the provided fields (First Name, Last Name, Email Address)
- Entity will review the provided names prior submission to ensure all participants are active employees and reasonably expected to be working during ISA assessment period
  - Replace submissions for employees that do not meet the criteria

- The submitted entries must include 3 executives, 3 IT administrators, and the remaining users a mixture from all entity's business units
    - If entity has less than the minimum required employee classes for any given category, all employees in the category will be provided
- The CIO, AIO, SCM, and other key role team members will be excluded from the submitted entries
- Entity must Whitelist the CND phishing server IP addresses, see Appendix F of this guide for instructions
    - Entities not on O365 email must seek assistance with the vendor to ensure they whitelist the provided email server prior to the assessment period
    - Failing to Whitelist the server or blocking (manually or automated) the phishing server will result in an automatic score of Non-Compliance for violation of the Rules of Engagement

Penetration Test Team Spear-Phishing Event/Tasks: Pen Test Team events are designed to test the entity's currently deployed security tools and assess their ability to detect and prevent malware payloads, malicious process execution, and Command and Control (C2) network communications. These events may include specially crafted payloads designed to emulate a threat actors attempt to compromise credentials and establish a backdoor into the internal entity network. Any achieved call-back from the entity network reports directly to a CND controlled command and control server. These actions are designed to test security controls implementation and are designed to dissolve at the end of the engagement, no manual clean-up should be required. Entities are prohibited from disabling, reimaging, or otherwise negatively impacting users who execute these payloads. It is both unnecessary and operationally disruptive.

The Pen Test Team Leader select users for the penetration test phishing from the users identified during the open-source data collection phase. As a result, selected users are likely different from those submitted for the RA Team Phishing Campaign.

Rules of Engagement

Expectation upon receipt of a Phishing Email during the Assessment Period: To ensure the entity both preserves the integrity of the assessment while appropriately defending their network, the following Rules of Engagement (RoE) are provided.

- All actions during the assessment period regarding possible phishing events require interaction with the CND prior to action.
- Under no circumstances will the entity block any identified CND Domains or IP addresses or report these addresses / IPs to 3rd party spam or Virus Total services!
    - This includes the automated reporting directly to 3rd party services
    - *If currently implemented in the entity environment*; Seek assistance from your supporting vendor to implement an identify and hold within an entity designed Phishing / Cybersecurity manager-controlled inbox
        - Held messages will undergo review as identified about prior to release if not CND sourced
    - Compliance failure will result in additional charges for reacquisition of new domains, reprogramming costs associated with designing new campaigns, lost usage time, and contacting costs
- During the *entire ISA period*, the entity shall report all detected instances of Phishing immediately to the RA Team, see above.
- Should an entity block a CND RA Team phishing attempt accidentally, due to configuration failure, or via automated measures, this will be considered a failure to follow the Rules of Engagement (RoE) for Phishing during the assessment will result in a false negative result and a non-compliance score for the impacted event.
- Improper actions regarding CND generated phishing message handling may result in a Failure of the measured task. CND recommends the entity refer to the Phishing Detection Workflow provided

below for additional assistance.

Risk Analysis Team Phishing

Warning -- RA Team phishing will be logged, and no other action taken. User inquiries will be provided the response “We are researching this issue; you may delete the email from your inbox”. No other actions or notifications will be undertaken until the end of the assessment period.

Warning – The entity is prohibited from notifying the participants of the Assessment Phishing Campaign while it is in process. Notifying users will result in a *Non-Compliance (N)* score for the associated event.

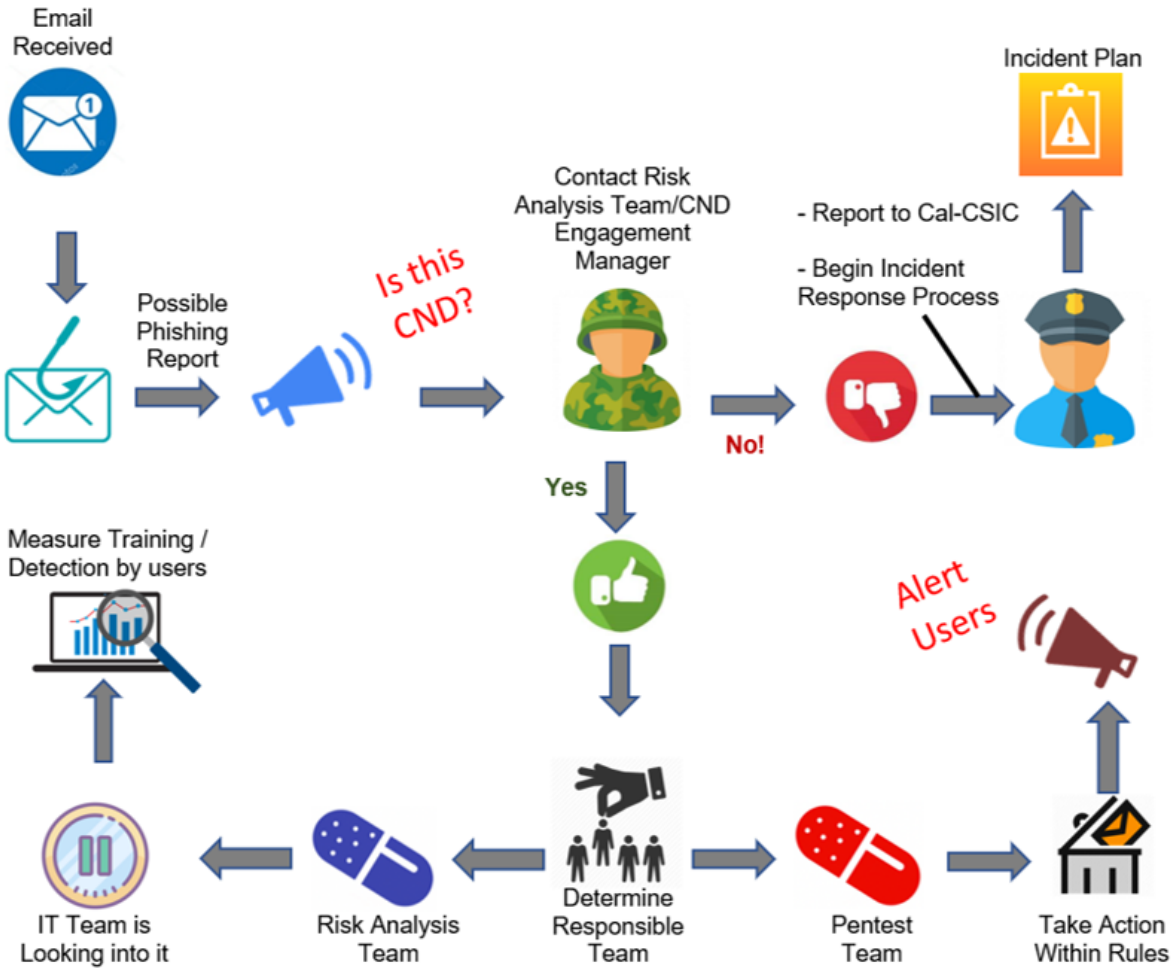
Penetration Test Team Phishing

Entity is authorized to take any of the following actions once a Pen Test Team spear-phishing attempt is identified:

- Notify users: Use preexisting documented notification procedures
- Email Removal: Remove the email using preexisting documented procedures
- **Do Not** require the host to be disabled, off lined, or otherwise reimaged. CND C2 malware is strictly controlled by the CND and safe for ISA use.
- **Do Not** submit samples using manual or automated methods to sandboxing, Malware Analysis, or other defensive tools / sites
- **Do Not** submit a report to any external Agencies, CDT (via Cal-CSIRS), or the Cal-CSIC, doing so expends efforts and takes time away from responses to real-world attack
- If external reporting is a part of your existing process, perform a tabletop exercise to discuss the actions with your team that you would normally take when reporting the event to the RA Team

Verified External Threat Actor generated events will be handled in accordance with the entity’s protection policies and reported through Cal-CSIRS.

Phishing Detection Workflow



Rules:

- Do not notify users if phishing is from Risk Analysis Team; responded to questions with "We're researching and will get back to you"
- Do not globally remove Risk Analysis Team phishing emails from users' boxes
- Do not globally block domains, senders, or web pages from users (either team)
- Do not submit attachments or domains to Cloud or on-premise cyber threat-intelligence feeds or Virus Total-like websites
- Do not open a Cal-CSIRS ticket if from either the Risk Analysis or Pentest teams.
- If you are not sure how to react, ask your onsite Risk Analysis Team or contact CND Engagement Manager for guidance

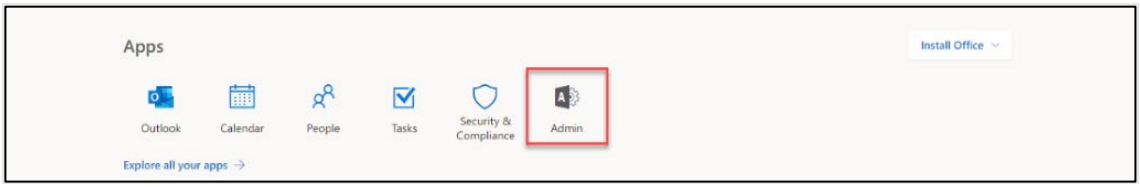
Appendix F - Phishing Whitelisting Procedures

Office 365 Whitelist Phishing Server IP Assessment

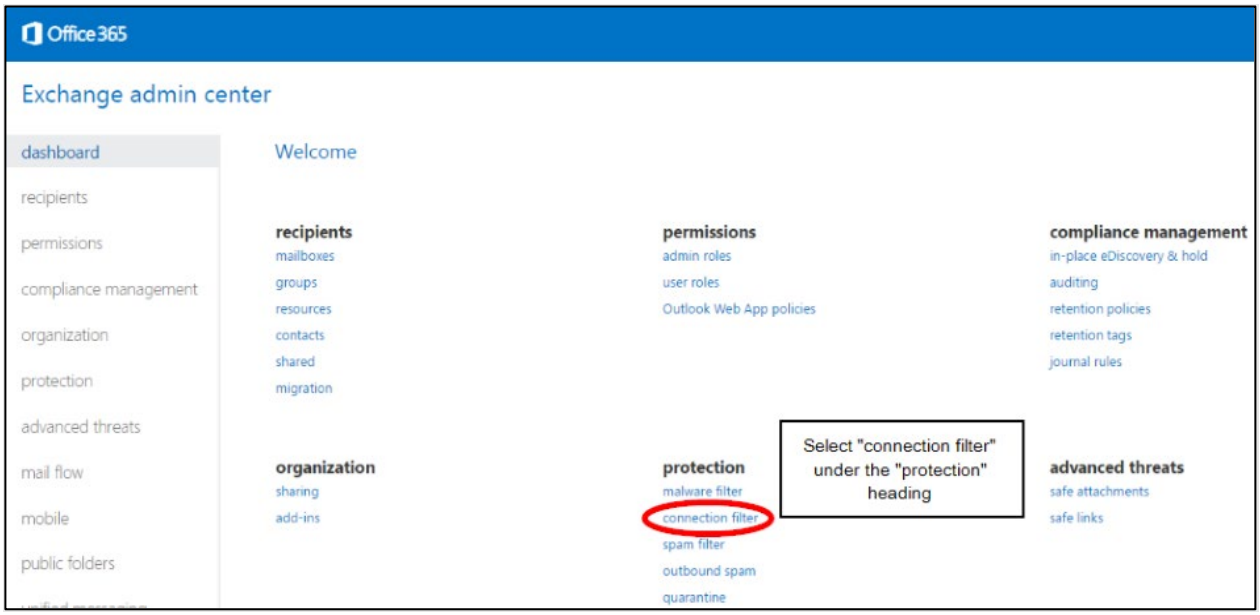
Note: Due to the nature of O365 updates, these screens may change without notice.

Setting Up Your IP Allow List

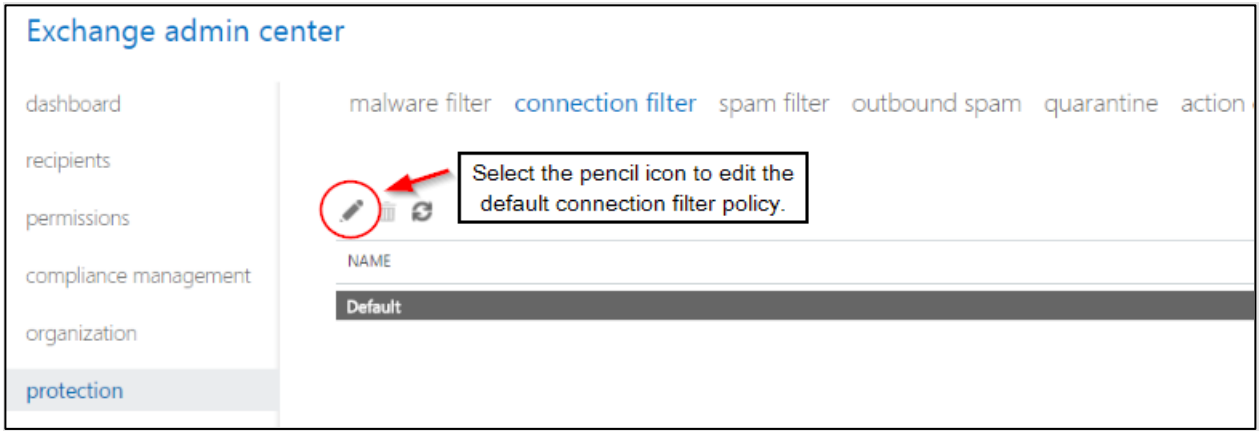
1. Log into your mail server admin portal and go into the **Admin -> Exchange.**



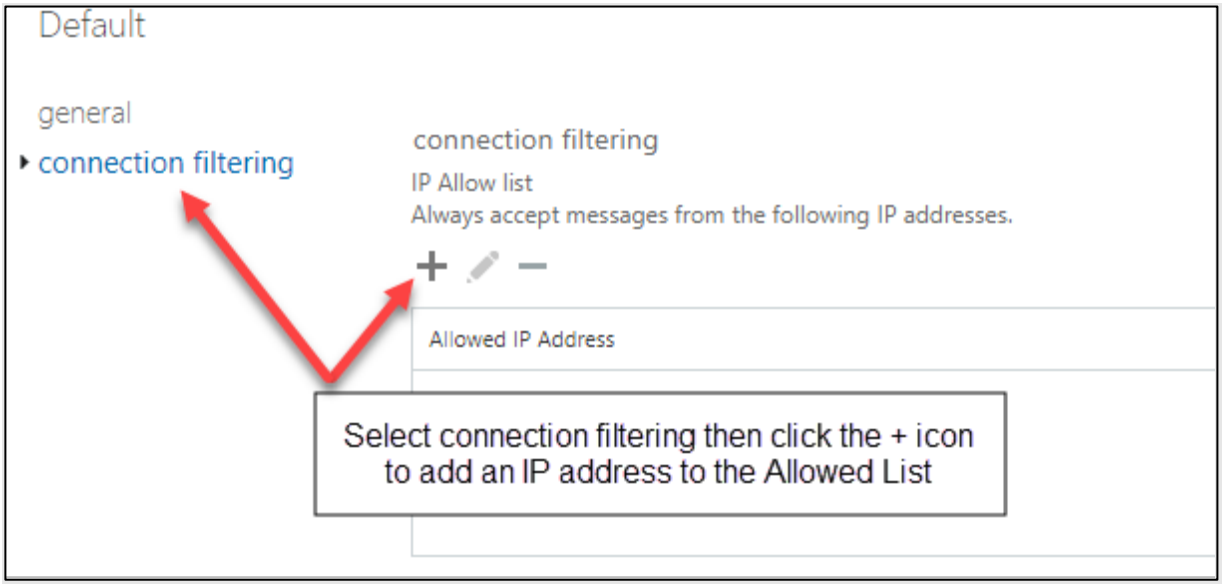
2. Click on **connection filter** (beneath protection heading).



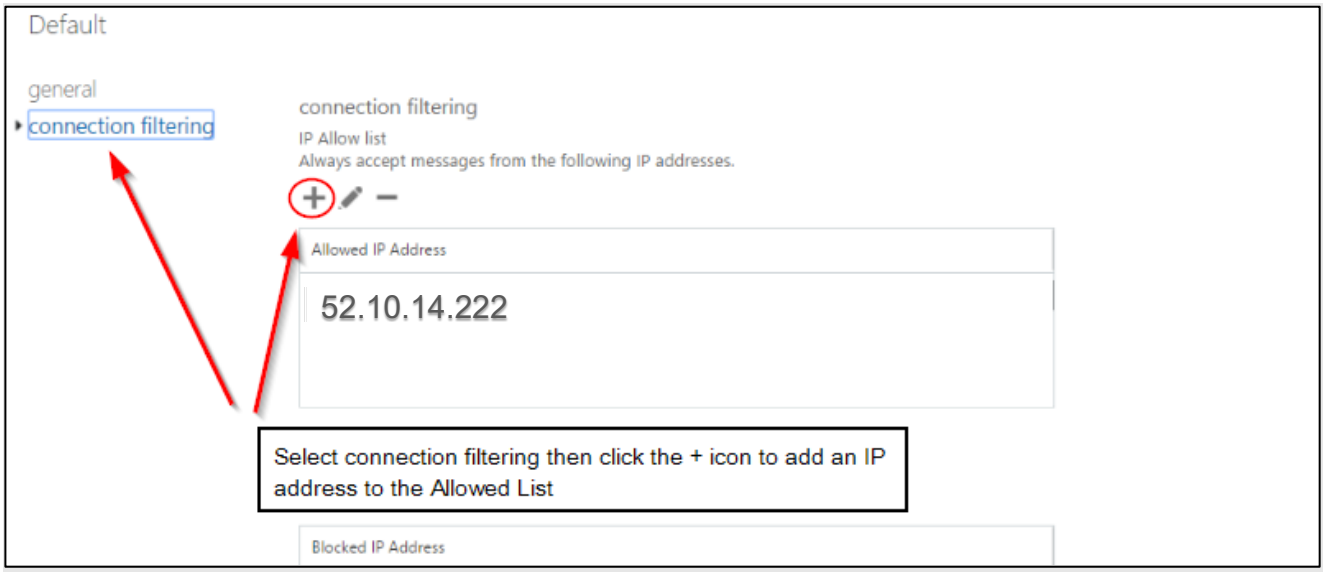
3. Click on **Connection Filter**, then the Pencil icon to edit the default connection filter policy.



4. Under the IP Allow list, click the + sign to add an IP address.



5. Under the **IP Allow list**, click the + sign to add an IP address

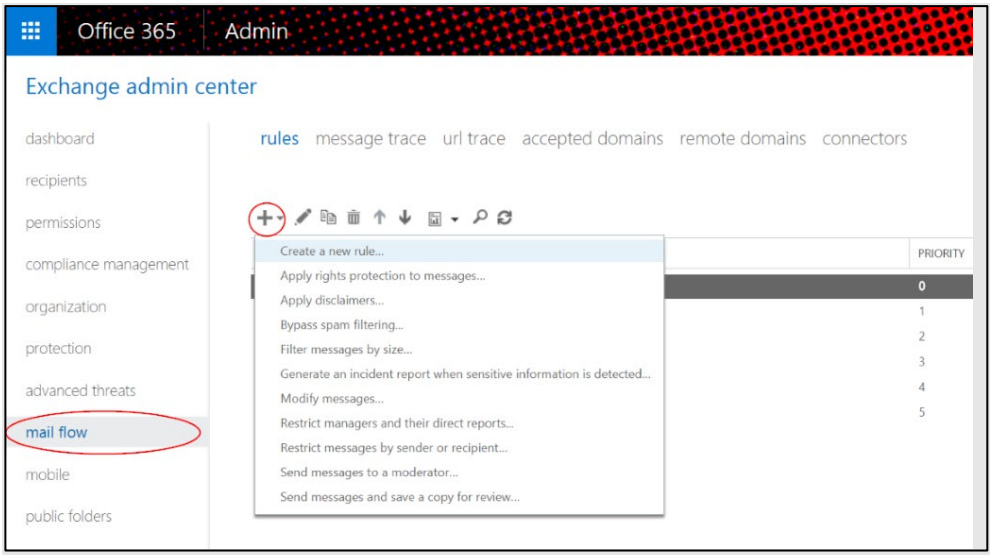


6. On the **Add allowed IP address** screen, add the following IP address
    a. 52.10.14.222

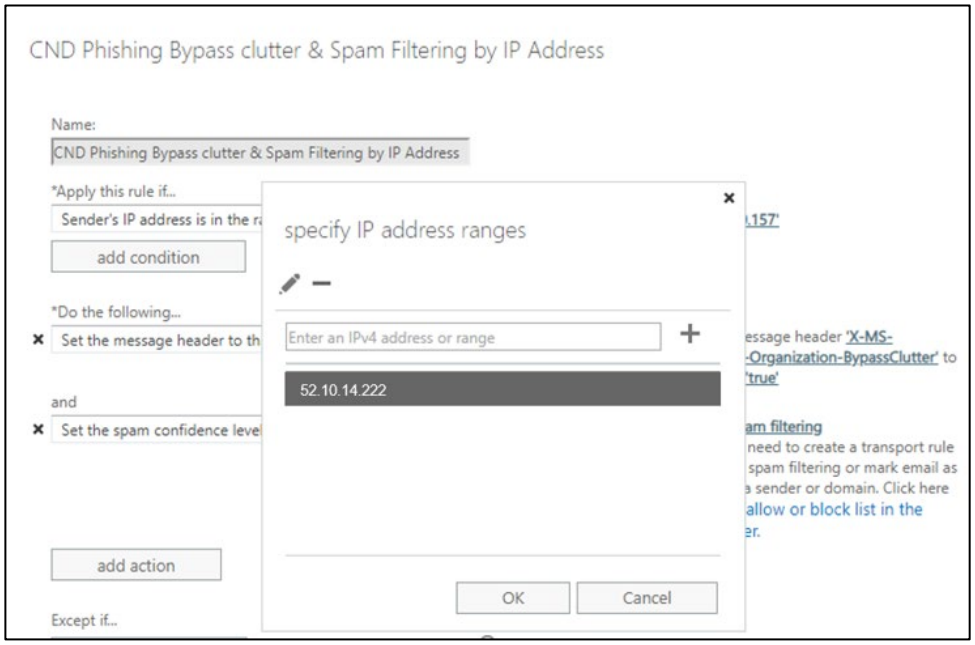
7. Click **OK**, then **Save**. Next, you will want to set up a mail flow rule to allow our mail to bypass spam filtering and the Clutter folder.

Bypass Clutter and Spam Filtering

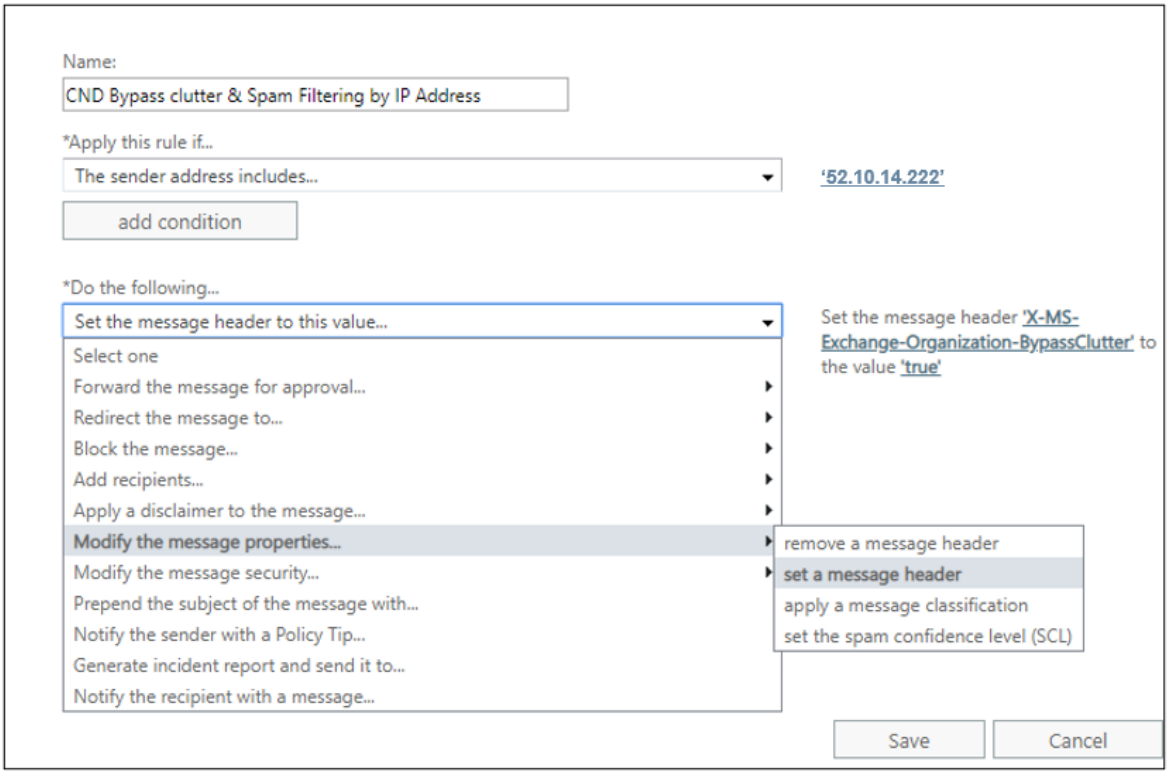
1. Go to **Admin** > **Mail** > **Mail Flow**.
2. Click the (+) Create New Rule button beneath **Mail Flow** > **Rules** > **Create a new rule…**



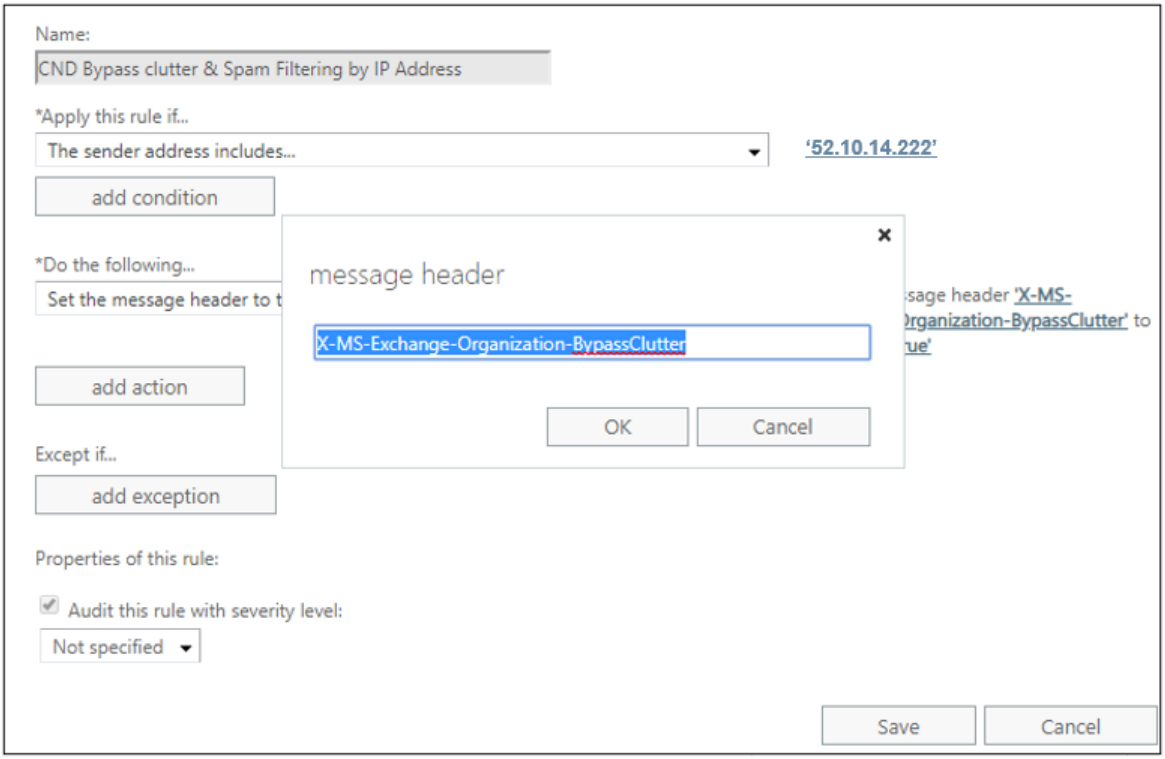
3. Name the rule **CND Phishing Bypass Clutter & Spam Filtering by IP Address.**
4. Click on **more options.**
5. Add the condition **Apply this rule if…**
6. Select **The sender address includes…**
7. Specify the IP address 52.10.14.222, then click **OK**:



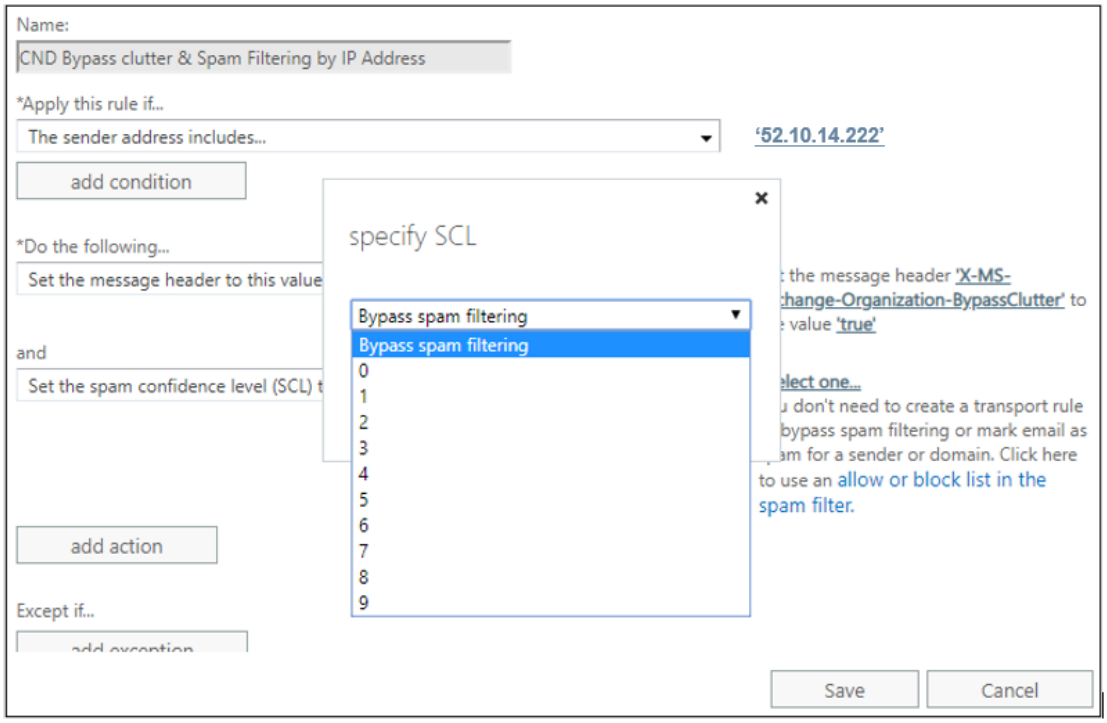
8. Beneath **Do the following,** click **Modify the message properties** then **Set a Message Header.**



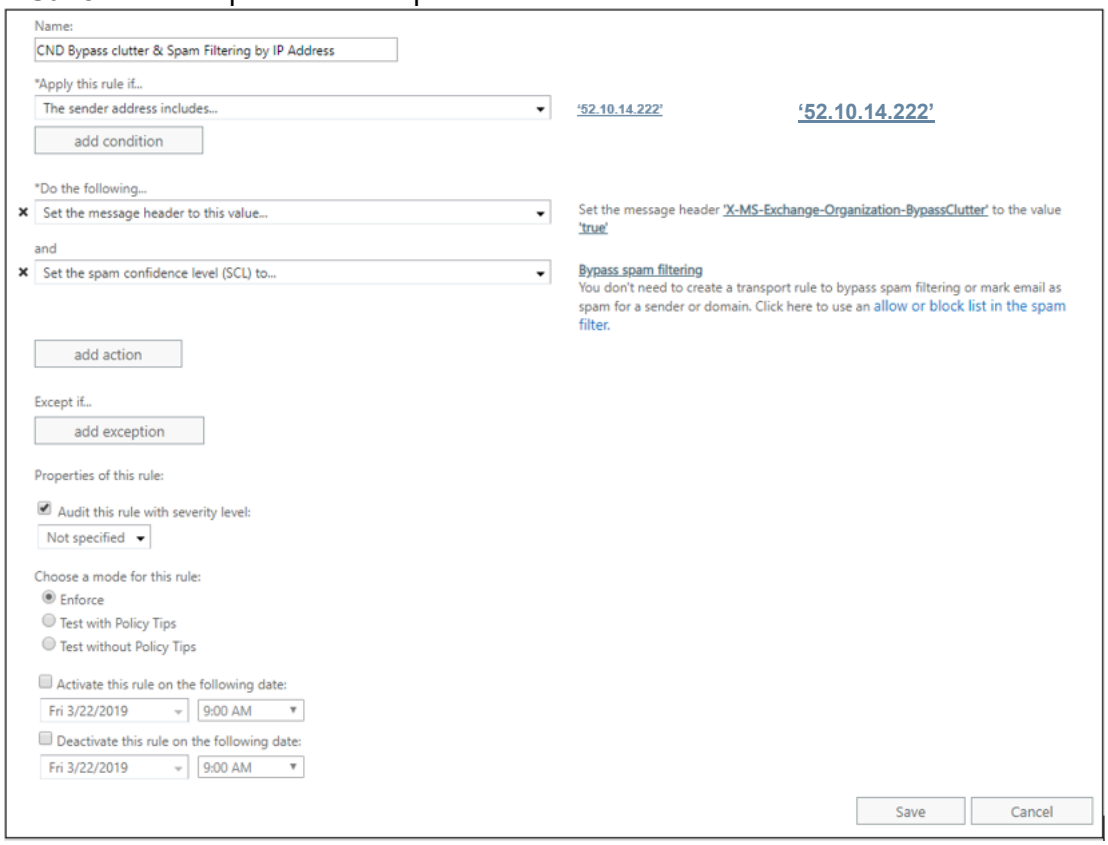
9. Set the message header to " **X-MS-Exchange-Organization-BypassClutter**" to the value "**true**"



10. Add an additional action beneath **Do the following to Modify the message properties**. Here, click on **Set the spam confidence level (SCL) to...** and select **Bypass Spam Filtering.**

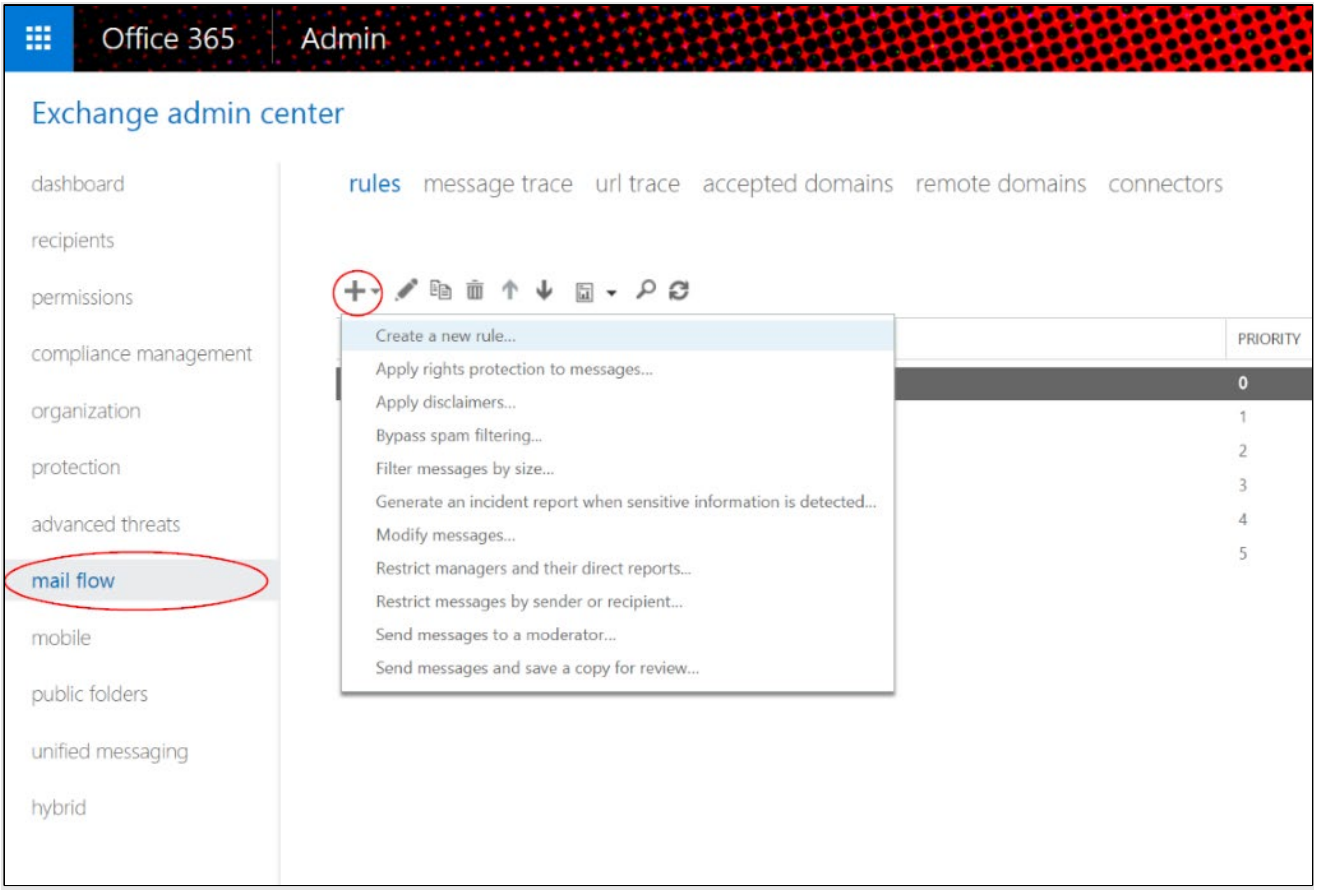


11. Click **Save**. An example of the completed rule is below.



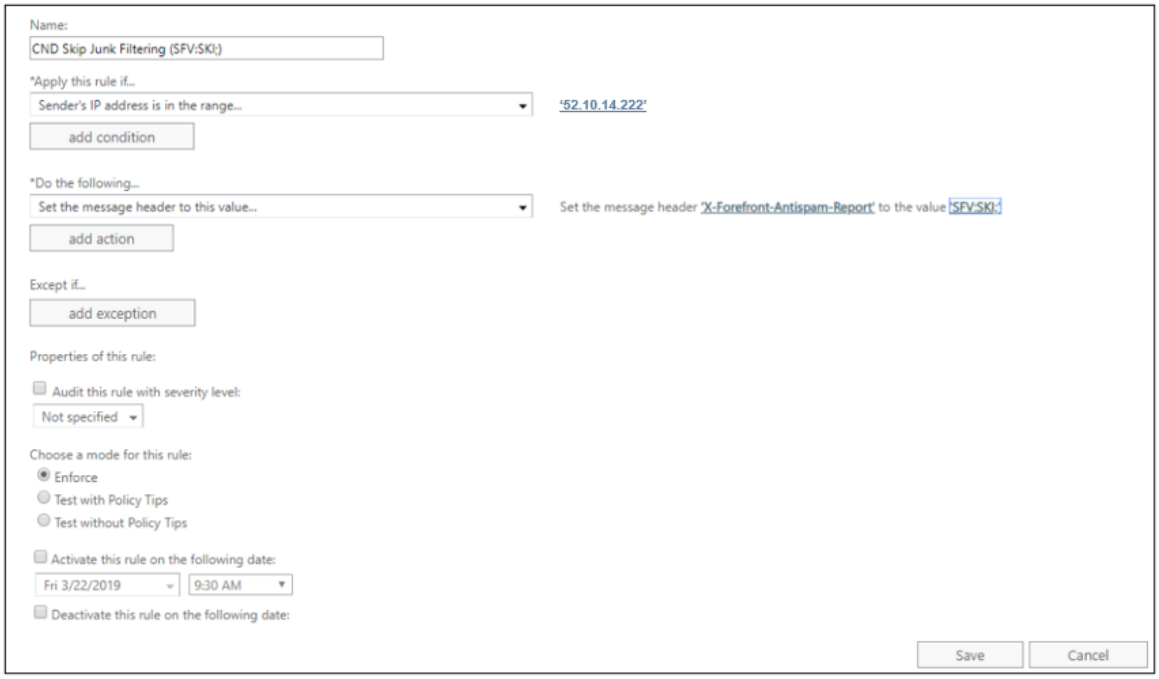
Bypassing the Junk Folder (O365 mail servers ONLY)

1. Go to **Admin > Mail > Mail Flow**.
2. Click the (+) Create New Rule button beneath **Mail Flow > Rules.**



3. Give the rule a name, such as "CND-Skip Junk Filtering".
4. Click on **More options.**
5. Add the condition **Apply this rule if.....**
6. Select **The sender**, then click on **More options** and select **IP address is in any of these ranges or exactly matches**. Specify the following sender IP address: 52.10.14.222, then click OK.
7. Beneath **Do the following:** click **Modify the message properties** then **Set a Message Heade**r.
9. Set the message header "**X-Forefront-Antispam-Report" to the value**" to the value "**SFV:SKI;**".
10. Beneath **Properties of this rule** set the priority to directly follow the existing rule (outlined in Bypassing Clutter and Spam Filtering) set up for CND whitelisting.

11. Click **Save**. An example of the completed rule is below.



Whitelist Phishing Server in URL Filtering Appliance

1. Please whitelist 52.183.38.170 in your URL filtering appliance. The links inside the phishing email will resolve to this IP. This will ensure that any links users click on will get through to record the results.

References

1. https://search.arin.net/rdap/?query=52.10.14.222
3. https://search.arin.net/rdap/?query=52.183.38.170
4. https://tlfhosting.com/

Additional Information

The two IP addresses identified in this Guide are used by the CND as part of its phishing campaign.

- 52.10.14.222 is an Amazon Web Service (AWS) IP that is used by The Linux Fix hosting provider that we use for hosted DNS/domain presence.
- 52.183.38.170 is an IP address assigned to us from Azure for our phishing server.

Under no circumstances, is the entity allowed to block these IP's or any domains associated with the campaigns.

Appendix G – Team Introduction Meeting Deliverables

The ISA process includes numerous sub-processes. Some sub-processes require documentation be obtained by the entity prior to commencement. This section identifies the documentation to be provided to the RA Team during the Team Introductions.

Purpose: Identify the minimum and optional documentation required to be presented to the CND RA Team upon start of assessment.

- The following Documentation must be provided. These can be provided via Entity SharePoint, Share folder or Entity provided USB:
  - RA Team credentials created for the assessment
  - RA Team IP address assignments
  - 10 IP / Hosts identified for System Hardening Testing
  - Network Interconnection Diagram
  - Data Call Worksheet (latest version if changes were made post submission) (or email to info@cnd.ca.gov) **Note:** *Entity MUST NOTIFY CND* no Less than 7 days prior of requested Data Call Changes for review prior to assessment.
  - All 3rd Party Pentest approval notices, response letters
- The following Optional Documentation (As applicable):
  - Any planned down time or maintenance windows that will impact the assessment period

Appendix H - Microsoft Teams Pre / Post Assessment Briefing Instructions

To reduce the impact on supported entities, the CND delivers the pre-assessment and post-assessment briefings over Microsoft Teams. This provides the assessed entity the maximum opportunity for participation by distributed team members. This model supports the State mandated migration to Office 365 and simplifies the installation of supported application tools within entity environments. To facilitate success, see the provided information below.

Preparing for Meetings (24 hours prior)

1) Download Microsoft Windows application/desktop client: Desktop clients can be downloaded and installed by end users directly from https://teams.microsoft.com/downloads if they have the appropriate local permissions (admin rights are not required to install the Teams client on a PC but are required on a Mac).

2) Join online: browser window will open with a prompt to enter name. Type name and select "Join Now" to test your connection to the meeting invite.

Attending a Meeting

The entity SCM which is typically the CIO or ISO, will receive an email invitation to the briefing.

1) Entity SCM should coordinate the location for their internal team members (e.g., conference room with computer projection resources) that will support as many co-located participants per connection as possible. If remote participants will be included, the CND requests the POC make distribution of the invitation to ensure only entity designated team members attend.

   ***Note*:** Due to the sensitive nature of this briefing, the entity is responsible to ensure only authorized participants attend. This is best controlled through single site participation.

2) If using the application, ensure the Microsoft Teams desktop client is installed on the conference computer. This may require prior coordination for assistance from the support desk.

3) To launch the meeting click on the "Join Microsoft Teams Meeting" link in the Calendar invite provided.

4) The link will open in a browser window with option to join the meeting, download the Windows app or join on the web instead. If you have already downloaded the app, you can use the "Launch it now" link.

   a) Join on the web instead: type your name in the prompt and select Join now. Ensure that the "Audio off" is enabled. A window will appear with "Hey (name), someone in the meeting should let you in soon". A CND member will grant access to guests.
   b) Launch it now: On the Microsoft Teams app will open and prompt you to select your audio and video settings for the meeting. Please ensure Audio is off and select the "Join now" button.

If you are having trouble connecting, please call the CND Engagement Manager at (916) 854-4CND (4263) to assist you in troubleshooting the issue.

Note: If your entity does not allow Microsoft Teams meeting within the environment, then you will need to host all meetings using your teaming application and provide presenter rights to the CND prior to meeting kick-off. Please coordinate this with the CND Engagement Manager immediately.

Appendix I - Links and Resource Pointers

Online resources

	Resource	Full Web Address
1	CDT IT Services Portal (ServiceNow) *	https://services.cdt.ca.gov/csm
2	CDT Independent Security Assessment Portal	https://cdt.ca.gov/security/independent-security-assessments-services/

CDT IT Services Portal (ServiceNow)*: Requires an account to be provisioned by CDT for system access. Please contact your agency's CDT account representative for assistance.

CND Point of Contact

For all ISA-related coordination and technical questions:

Name	Email	Phone
Alice Allersmeyer	info@cnd.ca.gov	(916) 854-4CND (4263)

CDT Point of Contact

Name	Email	Phone
Helen Woodman	helen.woodman@state.ca.gov	(916) 431-4698