



**ACHD**  
ASSOCIATION OF CALIFORNIA  
HEALTHCARE DISTRICTS

**Association of California Healthcare Districts**  
Governance versus Management/Staff Matrix of Responsibilities

**Strategy**

Responsibility	Board Role	Management Role
<b>Development and Review of Mission, Values and Vision</b>	<ul style="list-style-type: none"> <li>Approves and helps formulate</li> <li>Participates in annual strategic planning that reviews and updates the statements, when necessary</li> </ul>	<ul style="list-style-type: none"> <li>Provides input and background material for board review and discussion prior to formulating and/or updating the statements</li> </ul>
<b>Implementation of Mission, Values and Vision</b>	<ul style="list-style-type: none"> <li>Makes decisions that support the mission, values, and vision</li> </ul>	<ul style="list-style-type: none"> <li>Establishes and carries out strategies aligned with mission, values and vision</li> <li>Sets the tone and expectations for the culture of the association</li> </ul>
<b>Long-Term Strategic Plan</b>	<ul style="list-style-type: none"> <li>Exhibits leadership in strategic thinking and planning sessions, reviewing relevant materials, and engaging in robust debate and dialogue about critical issues impacting association</li> <li>Determines strategic directions, including strategic initiatives that address membership needs</li> <li>Approves the long-term strategic plan</li> </ul>	<ul style="list-style-type: none"> <li>Enables well-informed, data-driven board discussions, debate, and decision-making by providing relevant data, information and background materials and input</li> <li>Develops strategic recommendations, measurable objectives, action plans and budgets to support and implement strategic goals and directions</li> </ul>
<b>Short-Term Plans</b>	<ul style="list-style-type: none"> <li>Ensures progress towards goals through regular monitoring and oversight</li> </ul>	<ul style="list-style-type: none"> <li>Develops and implements plans</li> </ul>
<b>Monitoring Strategic Progress</b>	<ul style="list-style-type: none"> <li>Regularly reviews progress</li> <li>Asks probing questions to ensure board member understanding and progress towards goals and objectives</li> <li>Advises and collaborates with management on corrective measures, as appropriate</li> </ul>	<ul style="list-style-type: none"> <li>Defines measures for tracking performance</li> <li>Reports measures to the board, interprets meaning and identifies barriers or challenges to success</li> </ul>
<b>Day-to-Day Operations</b>	<ul style="list-style-type: none"> <li>No role</li> </ul>	<ul style="list-style-type: none"> <li>Makes all management decisions</li> <li>Develops policies and procedures</li> <li>Advises board, as appropriate</li> </ul>

## Leadership Structure and Governance Processes

Responsibility	Board Role	Management Role
<b>Board Roles, Responsibilities and Composition</b>	<ul style="list-style-type: none"> <li>Clearly defines the board and committee roles in written documentation</li> <li>Ensures leadership qualities, background, and knowledge is in place for effective governance</li> <li>Establishes and uses board committees effectively</li> </ul>	<ul style="list-style-type: none"> <li>Provides information, resources, and opportunities for board use in strengthening their effectiveness</li> <li>Tracks and reports on board composition to ensure that it reflects a diversity of the membership</li> </ul>
<b>Board Reports</b>	<ul style="list-style-type: none"> <li>Evaluates information reported, engaging in appropriate strategic-level dialogue</li> <li>Accepts and approves reports</li> </ul>	<ul style="list-style-type: none"> <li>Prepares concise reports and well-conceived recommendations for board consideration</li> </ul>
<b>Strategic Focus and Discussion</b>	<ul style="list-style-type: none"> <li>Discussions focus on the board's policy-making function, rather than operational thinking or decision-making</li> <li>Ensures most of the meeting time is spent on strategic issues</li> <li>Engages in lively dialogue that is respectful and includes participation from all</li> </ul>	<ul style="list-style-type: none"> <li>Focus on operational thinking and decision-making, using the board's policy-making and strategic leadership as a guide</li> </ul>
<b>Board Policies and Procedures</b>	<ul style="list-style-type: none"> <li>Uses governance policies and procedures to clearly define the board's responsibilities, delineating between board, management, and staff</li> <li>Uses policies and procedures to establish efficiency and consistency</li> <li>Reviews board structure, committee practices, tenure, policies, and bylaws regularly</li> </ul>	<ul style="list-style-type: none"> <li>Drafts strong, well-written policies for board review and approval</li> <li>Facilitates a process for periodic policy review, update, and approval</li> </ul>
<b>Board Performance</b>	<ul style="list-style-type: none"> <li>Board members are well-prepared at every meeting to engage in meaningful discussion and decision-making</li> <li>A regular board practices and performance self-assessment is conducted, and the board takes corrective action for improvement, when appropriate</li> </ul>	<ul style="list-style-type: none"> <li>Ensures board members are provided with agendas, reports, and other relevant materials well-enough in advance of meetings to enable meaningful and efficient discussion and decision making</li> <li>Provides administrative assistance in conducting the board self-assessment</li> </ul>
<b>Executive Meetings</b>	<ul style="list-style-type: none"> <li>Used as appropriate to promote open communication between the board and CEO on serious or time sensitive issues</li> </ul>	<ul style="list-style-type: none"> <li>Develops agenda and materials for regularly scheduled meetings</li> <li>Requests special meetings as needed</li> </ul>

## Code of Conduct/Conflict of Interest

Responsibility	Board Role	Management Role
<b>Development and Implementation of a Code of Conduct and Conflict of Interest</b>	<ul style="list-style-type: none"> <li>• Adopts a Code of Conduct that each board member reviews annually</li> <li>• Annual statement of Conflict of Interests is distributed and signed by all board members</li> </ul>	<ul style="list-style-type: none"> <li>• Abides by the association's values and ethical principles, and demonstrates the values and ethics through personal actions as well as operational rules, policies, new employee orientation, training, and internal communications</li> </ul>
<b>Awareness of Conduct and Conflicts</b>	<ul style="list-style-type: none"> <li>• Ensures a process to allow confidential concerns about issues are brought to appropriate persons</li> </ul>	<ul style="list-style-type: none"> <li>• Takes the operational steps necessary to ensure that the board-approved ethical principles and values are provided to all individuals associated with the association</li> <li>• Develops and implements a process to allow confidential concerns about ethical issues to be brought to appropriate persons</li> </ul>



## Relationship with the CEO

Responsibility	Board Role	Management Role
<b>Board and CEO Roles</b>	<ul style="list-style-type: none"> <li>• Understands the board’s strategic/policy responsibilities vs. the CEO’s operational responsibilities</li> <li>• Adheres to the governing board’s policy-making role, and does not interfere in the CEO’s operations management role</li> </ul>	<ul style="list-style-type: none"> <li>• Understands the board’s strategic/policy responsibilities vs the CEO’s operational responsibilities</li> <li>• Expects the board to engage in deep probing dialogue about strategic issues rather than “rubber stamp” management proposals and ideas</li> </ul>
<b>Communication, Support and Shared Goals</b>	<ul style="list-style-type: none"> <li>• Consistently supports the CEO in the pursuit and implementation of board-approved objectives</li> <li>• Mutual trust and respect exist between board and the CEO</li> </ul>	<ul style="list-style-type: none"> <li>• CEO maintains a positive relationship and ongoing communication with the board, including between board meetings when necessary</li> <li>• Mutual trust and respect exist between board and the CEO</li> </ul>
<b>CEO Evaluation</b>	<ul style="list-style-type: none"> <li>• Establishes CEO performance criteria and evaluates CEO performance annually</li> <li>• Sets the CEO’s compensation               <ul style="list-style-type: none"> <li>▪ Has strong understanding of compensation structures, legal and regulatory requirements</li> <li>▪ Uses pre-defined expectations and performance targets tied to association performance in setting compensation incentives</li> </ul> </li> <li>• Regularly reviews the CEO’s compensation to ensure that it is reflective of compensation trends of associations with similar size and scope</li> </ul>	<ul style="list-style-type: none"> <li>• The CEO should know his or her evaluation criteria at the onset of the evaluation period, and the annual evaluation should not come as a surprise</li> </ul>

## Human Resources

Responsibility	Board Role	Management Role
<b>Personnel Policies</b>	<ul style="list-style-type: none"> <li>• Reviews and adopts at least every three years</li> <li>• Provides expertise and counsel upon request regarding human resource issues and policies</li> </ul>	<ul style="list-style-type: none"> <li>• Drafts policies and makes recommendations to the board, and administers adopted policies</li> <li>• Develops strategies and implements action plans for strengthening employee satisfaction</li> </ul>
<b>Staff Salaries and Benefits</b>	<ul style="list-style-type: none"> <li>• Approves budget, ensuring adequate resources are in place to assure a competent, high-quality workforce</li> </ul>	<ul style="list-style-type: none"> <li>• Develops compensation and benefits strategies</li> <li>• Approves job classifications, salary ranges and benefits programs with input and recommendations from supervisory staff</li> </ul>
<b>Hiring of Staff</b>	<ul style="list-style-type: none"> <li>• Knows potential areas of workforce needs for the association</li> <li>• Understands current and emerging barriers to recruitment, provides expertise and counsel in devising strategies to meet workforce needs</li> <li>• No role in hiring of individual personnel</li> </ul>	<ul style="list-style-type: none"> <li>• In conjunction with supervisory staff, hires and evaluates the people necessary to meet current and workforce needs</li> <li>• Along with supervisory staff, develops and implements new employee orientation and training</li> </ul>
<b>Staff Responsibilities and Job Assignments</b>	<ul style="list-style-type: none"> <li>• No role</li> </ul>	<ul style="list-style-type: none"> <li>• Administers staffing levels, job classifications, job descriptions, etc.</li> </ul>
<b>Staff terminations and reductions in force</b>	<ul style="list-style-type: none"> <li>• No role in individual terminations apart from senior staff. Shall be advised of executive staff terminations and shall provide counsel upon request</li> <li>• Is advised of expected reductions in force and understands the business needs, rationale, and implications for reductions</li> </ul>	<ul style="list-style-type: none"> <li>• Makes final termination decisions</li> <li>• Makes decisions regarding reductions in force</li> </ul>
<b>Staff Evaluation</b>	<ul style="list-style-type: none"> <li>• No role, with exception of CEO evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• Along with supervisory staff, is responsible for the staff's performance evaluation</li> </ul>

## Financial Leadership

Responsibility	Board Role	Management Role
<b>Budgeting</b>	<ul style="list-style-type: none"> <li>• Provides input and counsel to the CEO regarding budget assumptions and programmatic changes affecting the budget</li> <li>• Ensures adequate capital is available to achieve the plan</li> <li>• Approves the budget</li> </ul>	<ul style="list-style-type: none"> <li>• Develops policy on standardized budget procedures</li> <li>• Prepares a preliminary budget that will support implementation of the strategic plan</li> <li>• Develops assumptions, targets and objectives and makes recommendations to the board</li> </ul>
<b>Monitoring Financial Progress</b>	<ul style="list-style-type: none"> <li>• Identifies and approves performance targets</li> <li>• Reviews performance targets at least quarterly</li> <li>• Uses financial performance reports to modify assumptions and shifts resources, as necessary</li> <li>• Reviews and approves the annual audit</li> </ul>	<ul style="list-style-type: none"> <li>• Tracks detailed financial progress, and takes immediate corrective action when necessary</li> <li>• Develops financial reports for the board in an easy-to-understand format, highlighting major trends and key indicators</li> <li>• Stimulates robust discussion and dialogue that enables timely decision-making</li> </ul>
<b>Capital Purchases</b>	<ul style="list-style-type: none"> <li>• Evaluates and approves requests and recommendations for capital purchases</li> </ul>	<ul style="list-style-type: none"> <li>• Prepares substantiated requests and recommendations for capital purchases</li> </ul>
<b>Decisions on Building, Renovation, Leasing, Expansion</b>	<ul style="list-style-type: none"> <li>• Evaluates needs, proposals, and recommendations, makes decisions</li> </ul>	<ul style="list-style-type: none"> <li>• Conducts research, prepares reports and makes recommendations for board consideration</li> <li>• Exercises contractual authority</li> </ul>
<b>Dues Structure</b>	<ul style="list-style-type: none"> <li>• Reviews dues structure at least every three years</li> <li>• Evaluates recommendations from management and staff on modifications to the dues structure</li> <li>• Approves dues budget annually as part of the budget approval process</li> <li>• Approves any delay of dues collection as appropriate</li> </ul>	<ul style="list-style-type: none"> <li>• Makes recommendations to the board regarding a need for a dues structure modification</li> <li>• Oversees dues collection on an annual basis and reports to the board</li> </ul>

## Stakeholder/Policy Maker Communications

Responsibility	Board Role	Management/Staff Role
<b>Advocacy</b>	<ul style="list-style-type: none"><li>• Approves advocacy/political agenda as recommended by the ACHD Advocacy Committee</li></ul>	<ul style="list-style-type: none"><li>• Develops legislative/political strategies and recommends association's position</li><li>• Ensures board education and understanding of issues and facilitates board advocacy and communication with elected officials</li><li>• Is knowledgeable and well-informed regarding issues, conducts ongoing communication with elected officials</li></ul>



**ACHD Board of Directors Calendar of Time Sensitive Business**

*Commencing with the start of the fiscal year, July 1*

Time Frame	Action Items	Executive Committee	Board of Directors
July/August	<ul style="list-style-type: none"> <li>• Notice to the Board of Directors regarding Executive Committee vacancies expected in the coming year and information on the nomination process</li> </ul>	✓	
	<ul style="list-style-type: none"> <li>• Chair prepares officer slate for approval by the Executive Committee at the September meeting</li> </ul>	✓	
	<ul style="list-style-type: none"> <li>• In accordance with Board Policy 7, CEO Evaluation is to occur in the first quarter of the fiscal year.                             <ul style="list-style-type: none"> <li>○ CEO Evaluation tool to be distributed to the Board in July with a completion due date of July 15</li> <li>○ Walker Company to compile results and share with the Board of Directors</li> </ul> </li> </ul>	✓	✓
	<ul style="list-style-type: none"> <li>• Review Lincoln Financial 401K Trustee Designations and make changes if needed due to Board turn over</li> </ul>		✓
September	<ul style="list-style-type: none"> <li>• Board of Directors meets in closed session to discuss the results of the CEO Evaluation                             <ul style="list-style-type: none"> <li>○ Executive Committee meets in closed session with CEO to review evaluation results and makes determination on incentive pay</li> </ul> </li> </ul>	✓	✓
	<ul style="list-style-type: none"> <li>• Executive Committee approves and recommends officer slate to the Board of Directors for approval at the meeting prior to the ACHD Annual Meeting</li> </ul>	✓	
	<ul style="list-style-type: none"> <li>• Board of Directors approves officer slate for the upcoming year at the board meeting prior to the ACHD Annual Meeting</li> </ul>		✓
	<ul style="list-style-type: none"> <li>• Beginning in 2021, at a minimum, every three (3) years the Executive Committee reviews the ACHD Employee Handbook and makes any necessary recommendations regarding personnel policies</li> </ul>	✓	



October	<ul style="list-style-type: none"> <li>• Board of Directors Self-Assessment Tool Distributed to the Board with due date</li> </ul>		✓
December	<ul style="list-style-type: none"> <li>• Board of Directors discusses the results of the Board Self-Assessment and possible goals for the coming year based on these results</li> </ul>		✓
	<ul style="list-style-type: none"> <li>• Board of Directors reviews and accepts the annual audit</li> </ul>		✓
February	<ul style="list-style-type: none"> <li>• Board of Directors meets in person to participate in Strategic Planning Session and approves the final Strategic Plan, which then informs the upcoming fiscal year budget <ul style="list-style-type: none"> <li>○ Strategic Plan to includes goals set as a result of the Board Self-Assessment</li> </ul> </li> </ul>		✓
May	<ul style="list-style-type: none"> <li>• Board of Directors approves the annual budget</li> <li>• CEO Reports to the Board regarding the progress on the Strategic Plan and Supplemental CEO Goals</li> </ul>		✓



## Conflicts of Interest

The purpose of the Conflict of Interest Policy, as written in Article XIV of the Amended and Restated Bylaws (effective date, July 2, 2017) is to protect the Association when it is contemplating entering into a transaction or arrangement that might benefit the private interest of an officer or Director of the Association or might result in a possible excess benefit transaction. The conflict of interest policy set forth in this Article XIV is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to nonprofit and charitable organizations.

### Section 2. Definitions

The following capitalized words and phrases shall have the meanings indicated powers.

- A. "Committee Member:" A member of a committee with Board delegated
- B. "Interested Person:" Any Director, officer, or Committee Member, who has a direct or indirect financial interest, as defined below.
- C. "Financial Interest:" A person has a "financial interest" if the person or a member of the person's family, which shall include any brother, sister, ancestor, descendant, spouse, brother-in-law, sister-in-law, son-in-law, daughter-in-law, mother-in-law, or father-in-law of such person, has, directly or indirectly, through business or investment:
  - 1. An ownership or investment interest in an entity with which the Association has, or within the previous 12 months has had, a transaction or arrangement;
  - 2. A compensation arrangement with the Association or with any entity or individual with which the Association has, or within the previous 12 months has had, a transaction or arrangement;
  - 3. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Association is negotiating a transaction or arrangement; or
  - 4. Compensation includes direct and indirect remuneration as well as, scholarships, grants, gifts or favors that are not insubstantial.
  - 5. Notwithstanding the foregoing, (a) the payment of dues by a Member for which the Director is a trustee or senior officer does not constitute a financial interest, and (b) the Association's reimbursements or payments to Directors in connection with their Board service does not constitute a financial interest.
  - 6. A financial interest is not necessarily a conflict of interest. A person who has a financial interest may have a conflict of interest only if the Board or the appropriate committee decides that a conflict of interest exists.

### Section 3. Duty to Disclose

In connection with any actual or possible conflict of interest, an interested person must disclose the existence of the financial interest and be given the opportunity to disclose all material facts to the Directors and Committee Members considering the proposed transaction or arrangement.

#### **Section 4. Determining Whether a Conflict of Interest Exists**

After disclosure of the financial interest and all material facts, and after any discussion with the interested person, he/she shall leave the Board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining Board or committee members shall decide if a conflict of interest exists.

#### **Section 5. Procedures for Addressing the Conflict of Interest**

- A. An interested person may make a presentation at the Board or committee meeting, but after the presentation, he/she shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.
- B. The chairperson of the Board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.
- C. After exercising due diligence, the Board or committee shall determine whether the Association can obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.
- D. If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the Board or committee shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in the Association's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination, it shall make its decision as to whether to enter into the transaction or arrangement.

#### **Section 6. Violations of the Conflicts of Interest Policy**

If the Board or committee has reasonable cause to believe an officer, Director, or Committee Member has failed to discuss actual or possible conflicts of interest, it shall inform the officer, Director, or Committee Member of the basis for such belief and afford the officer, Director, or Committee Member an opportunity to explain the alleged failure to disclose.

If, after hearing the officer, Director, or Committee Member's response and after making further investigation as warranted by the circumstances, the Board or committee determines the officer, Director, or Committee Member has failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

#### **Section 7. Records of Proceedings**

The minutes of the Board and all committees with Board delegated powers shall contain:

- A. The names of the officers, Directors, or Committee Members who disclosed or otherwise were found to have a financial interest in connection with a conflict of interest as present, and the Board's or committee's decision as to whether a conflict of interest in fact existed.
- B. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection with the proceedings.

#### **Section 8. Compensation**

- A. A voting Director who receives compensation, directly or indirectly, from the Association for services is precluded from voting on matters pertaining to that Director's compensation.



B. A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Association for services is precluded from voting on matters pertaining to that officer's, Director's, or Committee Member's compensation.

C. No voting Director or any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirect, from the Association, either individually or collectively, is prohibited from providing information to any committee regarding compensation.

**Section 9. Annual Statements**

Each director, principal officer and Committee Member shall annually sign a statement which affirms such person:

**Article XIV**

- A. Has received a copy of this conflict of interest policy set forth in this
- B. Has read and understands the policy;
- C. Has agreed to comply with the policy; and
- D. Understands the Association is charitable and in order to maintain its federal tax-exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.

**Section 10. Periodic Reviews**

A. To ensure the Association operates in a manner consistent with charitable purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

B. Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining; and

C. Whether partnerships, joint ventures, and arrangements with management organizations conform to the Association's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further charitable purposes and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

**Section 11. Use of Outside Experts**

When conducting the periodic reviews as provided for in Article XIV, Section 10, the Association may, but need not, use outside advisors. If outside experts are used, their use shall not relieve the Board of its responsibility for ensuring periodic reviews are conducted.

---

Signature

Date

---

Printed Name



## Board Member Code of Conduct

The following Code of Conduct was adopted by the ACHD Board of Directors on April 28, 2014 to describe the expectations of each Board member during and after their service.

As a member of the ACHD Board of Directors I will:

- Represent the best interests of ACHD members and the association; Be a positive example to others in ACHD in both my attitude and actions, acting at all times with honesty, integrity, diligence, competence and in good faith;
- Become and stay knowledgeable about the Board's bylaws and procedures;
- Become well-informed about each matter coming before the Board for decision;
- Bring matters to the Board's attention that I believe may have a significant effect on the well-being of ACHD members or the association;
- Participate actively in Board and committee discussions;
- Listen carefully to other members and consider their opinions respectfully, particularly if they differ from mine;
- Respect and support majority decisions of the Board, even if I disagree with that result.
- Acknowledge conflicts that arise between my personal interests and the Board's activities, identifying them early and withdrawing from related discussions and votes;
- Maintain, in accordance with law, the confidentiality of information provided to me in my role as a Board Member;
- Refer member complaints promptly and directly to the Board Chair and appropriate Association staff.
- Surrender all information related to ACHD matters to my successor, but continue to maintain related duties of confidentiality.
- Comply with all ACHD policies and procedures to support a work environment that discourages any form of inappropriate conduct, harassment, discrimination, or retaliation;
- Recognize and respect the differentiation between board and staff responsibilities.

I will not:

- Share opinions elsewhere that I am unwilling to discuss before the Board or its committees;
- Decide how to vote before hearing discussion and becoming fully informed;
- Interfere with duties and activities of other Board members;
- Speak publicly on behalf of the Board unless specifically authorized to do so.

---

Signature

Date

Department of Homeland  
Security  
CISA  
Cybersecurity Assessment

Remote Penetration Test  
Out-Brief



— DRAFT —

Northern Inyo Healthcare  
District

(NINYHCD)

Sep 20, 2023

FOR OFFICIAL USE ONLY



# NOTICE:

The information that follows in this presentation is preliminary and is not fully validated or finalized. Engineers and managers are still in the process of analyzing this information and preparing findings. It is presented in its rough draft state and may be significantly modified prior to the publication of the final report or an official out-brief.

This RPT is not an audit. The services provided only demonstrates what actions an adversary could accomplish within the timeframe of the assessment.



# Agenda

- Assessment Timeframe & Team
- Scope and Limitations
- Targets and Status
- Goals
- Open-Source Information Gathering
- Findings
- Observations
- Next Steps
- Questions



# Assessment Timeframe & Team

Date	Activity
2023-08-29 to 2023-09-08	External Assessment

## Customer Point of Contact (POC)

Dean Lewis	dean.lewis@nih.org
------------	--------------------

## RPT Fed Lead

Bob McNeal	robert.mcneal@cisa.dhs.gov
------------	----------------------------

## RPT Team

Blake Rash	
------------	--





# Scope and Limitations

- External IP Ranges
  - 66 IP addresses across a single (/26) subnet (and a few additional systems)
- Testing Limitations
  - Short timeframe - overcome by working with NINYHCD staff
  - Testing assumes in-scope systems are a fair representation of all production systems





# Goals

# Goals

- Identify risks within the environment
- Provide an actionable report that will increase security posture
- Identify specific external attack vectors that can be used to compromise assets
- Determine extent of possible compromise utilizing existing vulnerabilities



# Open-Source Information Gathering

- 38 emails were scraped from various Internet sources
- 37 scraped emails were identified as existing in previous data breaches (according to HaveIBeenPwned database)
- 37 sets of credentials (emails and passwords) identified in the wild
- 0 sets of credentials were successfully validated







# Findings

# Finding Severity Classification

Severity	Description
Critical	Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and/or potential severe impact. Critical items will be brought to the customer's attention immediately.
High	Intruders may be able to exercise full control on the targeted device such as: <ul style="list-style-type: none"><li>- Easily exploitable vulnerabilities that can lead to complete application, system and/or network compromise, such as an intruder having the ability to remotely administer files on a web server</li><li>- Severe router/firewall/server misconfigurations</li><li>- Worm, Trojan and/or backdoor detected</li><li>- Vulnerability exists that has tools readily available on the Internet to take advantage of it</li><li>- Weak passwords for remote administration and users</li></ul>
Medium	Intruders may be able to exercise some control of the targeted device such as: <ul style="list-style-type: none"><li>- Disclosure of unauthorized sensitive customer information or user account information</li><li>- An intruder can obtain full read access to corporate confidential information</li><li>- Lack of basic logging and alerting capabilities</li><li>- Antivirus misconfigurations</li><li>- Untrusted networks having access to trusted networks</li></ul>
Low	Vulnerabilities discovered and reported as item of interest, but are not normally exploitable. Many low items reported by security tools are not included in this report as they are often informational, unverified, or of minor risk.
Informational	Potential weaknesses within the system that cannot be readily exploited. These findings represent areas that the customer team should be cognizant of, but does not require any immediate action.



# Findings Overview

-- PRELIMINARY --

## Medium

- Unsupported SSL/TLS Encryption Cipher
- Spear Phishing Weaknesses

## Low

- Data Disclosure

## Informational

- Exposed Administrative Interface
- Self-Signed Certificates



# Medium

## Unsupported SSL/TLS Encryption Protocols

```
<ssltest host="162.252.88.34" sniname="162.252.88.34" port="4443">  
<protocol type="ssl" version="2" enabled="0" />  
<protocol type="ssl" version="3" enabled="0" />  
<protocol type="tls" version="1.0" enabled="0" />  
<protocol type="tls" version="1.1" enabled="1" />  
<protocol type="tls" version="1.2" enabled="1" />  
<protocol type="tls" version="1.3" enabled="1" />
```





# Low

## Data Disclosure

```
-----  
+ Target IP:          199.26.184.19  
+ Target Hostname:    webmail.nih.org  
+ Target Port:        80,443  
-----  
+ Server: Microsoft-IIS/8.5  
+ /: Uncommon header 'x-feserver' found, with contents: EX-MB-02  
+ /: The web server may reveal its internal or real IP in the Location header  
via a request to with HTTP/1.0. The value is "10.21.0.202". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649  
+ /Microsoft-Server-ActiveSync: Microsoft Exchange Systems (CAS and OWA) may  
reveal the internal or real IP in the WWW-Authenticate header via a request t  
o /Microsoft-Server-ActiveSync over HTTP/1.0. The value is "10.21.0.202". See  
: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
```



# Informational

## Self-Signed Certificates

```
SCAN RESULTS FOR MSGCTR.NIH.ORG:8010 - 199.26.184.18
-----

Certificate #0 ( _EllipticCurvePublicKey )
SHA1 Fingerprint:      1e9948d1f6e0bacb95255289292e7ae4361a5854
Common Name:          msgctr.nih.org
Issuer:               FGVMO4TM19002694
Serial Number:       198895222161669885742091
Not Before:          2022-10-04
Not After:           2023-10-17

Certificate #0 - Trust
Hostname Validation:  OK - Certificate matches server hostname
Android CA Store (13.0.0_r9):  FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Apple CA Store (iOS 16, macOS 13)  FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Java CA Store (jdk-13.0.2):      FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Mozilla CA Store (2022-12-11):    FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Windows CA Store (2023-02-19):    FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain

SCAN RESULTS FOR WEBMAIL.NIH.ORG:8010 - 199.26.184.19
-----

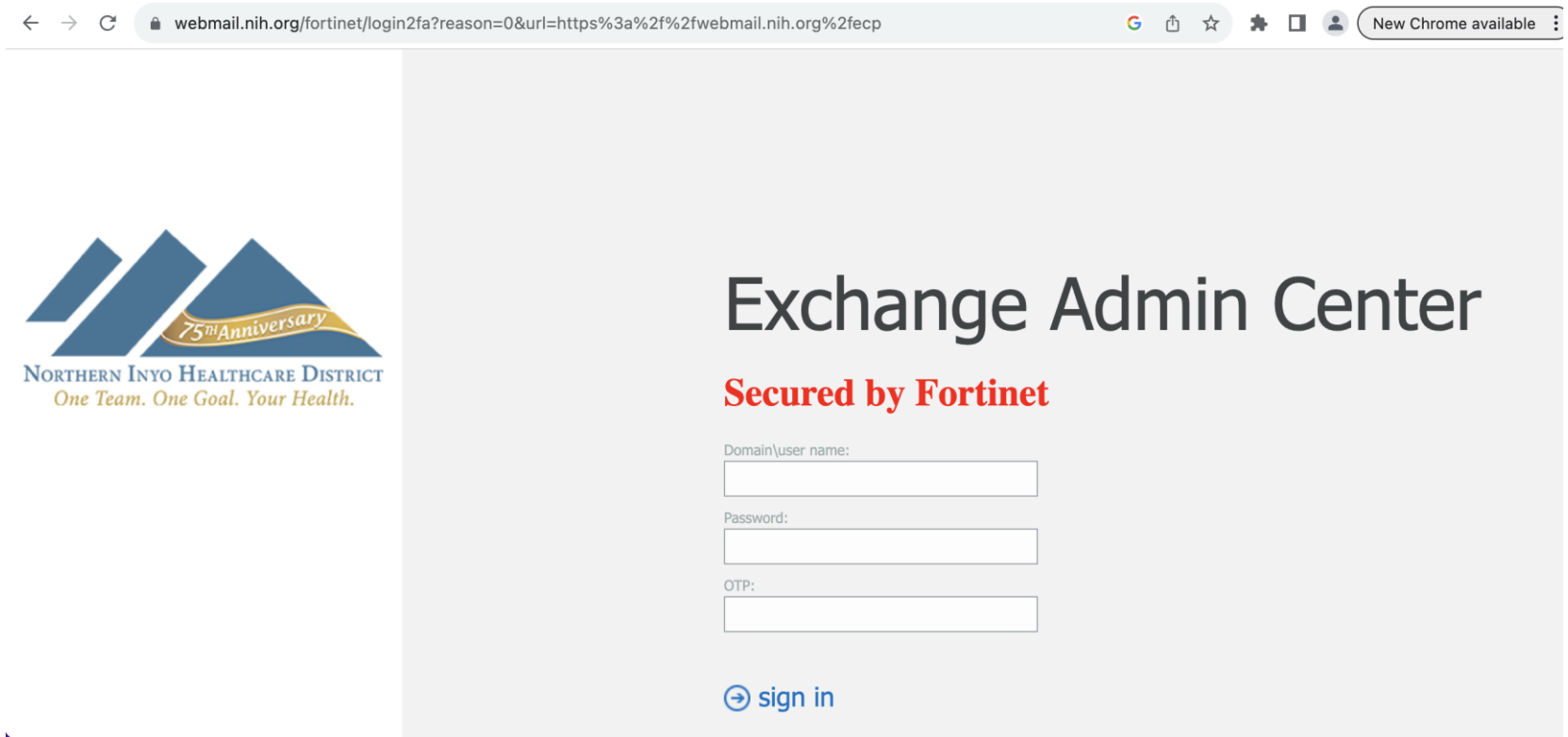
Certificate #0 ( _EllipticCurvePublicKey )
SHA1 Fingerprint:      ed8cf537aa5b692b557fecfd8fa647df0b926cca
Common Name:          webmail.nih.org
Issuer:               FGVMO4TM19002694
Serial Number:       51677996802764581530030
Not Before:          2022-10-04
Not After:           2023-10-17







Certificate #0 - Trust
Hostname Validation:  OK - Certificate matches server hostname
Android CA Store (13.0.0_r9):  FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Apple CA Store (iOS 16, macOS 13)  FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Java CA Store (jdk-13.0.2):      FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Mozilla CA Store (2022-12-11):    FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
Windows CA Store (2023-02-19):    FAILED - Certificate is NOT Trusted: self-signed certificate in certificate chain
```




# Informational

## Exposed Administrative Interface



← → ↻ [webmail.nih.org/fortinet/login2fa?reason=0&url=https%3a%2f%2fwebmail.nih.org%2fecp](https://webmail.nih.org/fortinet/login2fa?reason=0&url=https%3a%2f%2fwebmail.nih.org%2fecp)       New Chrome available



NORTHERN INYO HEALTHCARE DISTRICT  
*One Team. One Goal. Your Health.*

# Exchange Admin Center

**Secured by Fortinet**

Domain\user name:

Password:

OTP:

[→ sign in](#)



# Medium

## Spear Phishing Weaknesses

Payload	C2 Protocol	Border Protection	Host Protection
Linked VBScript HTA	DNS	Not Blocked	Blocked
Linked Tikitorch HTA	DNS	Not Blocked	Blocked
Linked Scarecrow	DNS	Not Blocked	Blocked
Linked Encrypted Macro Enabled Word Document	DNS	Not Blocked	Blocked
Linked Encrypted (Velvet Sweatshop) Excel Document	DNS	Not Blocked	Blocked



# Medium

## Spear Phishing Weaknesses

Payload	C2 Protocol	Border Protection	Host Protection
Linked Powershell HTA	HTTPS	Not Blocked	Blocked
Linked Morph Powershell HTA	HTTPS	Not Blocked	Blocked
Linked Sharpshooter HTA	HTTPS	Not Blocked	Blocked
Linked Sharpshooter HTA with ASMI Bypass	HTTPS	Not Blocked	Blocked
Linked Executable HTA	HTTPS	Not Blocked	Blocked
Linked VBScript HTA	HTTPS	Not Blocked	Blocked
Linked Cactustorch HTA	HTTPS	Not Blocked	Blocked
Linked Tikitorch HTA	HTTPS	Not Blocked	Blocked
Linked Tikitorch HTA (with 3 second delay)	HTTPS	Blocked	Blocked





# Medium

## Spear Phishing Weaknesses

Payload	C2 Protocol	Border Protection	Host Protection
Linked Scarecrow	HTTPS	Not Blocked	Blocked
Linked Bankai	HTTPS	Not Blocked	Blocked
Linked Executable	HTTPS	Not Blocked	Blocked
Linked Embedded LNK	HTTPS	Not Blocked	Blocked



# Medium

## Spear Phishing Weaknesses

Payload	C2 Protocol	Border Protection	Host Protection
Linked Macro Enabled Word Document	HTTPS	Not Blocked	Blocked
Linked Encrypted Macro Enabled Word Document	HTTPS	Not Blocked	Blocked
Linked Encrypted Macro Enabled Word Document (with 3 second delay)	HTTPS	Blocked	Blocked
Linked OLE Embedded Word Document	HTTPS	Not Blocked	Blocked
Linked Encrypted OLE Embedded Word Document	HTTPS	Not Blocked	Blocked
Linked Encrypted (Velvet Sweatshop) Excel Document	HTTPS	Not Blocked	Blocked



# Medium

## Spear Phishing Weaknesses

Payload	C2 Protocol	Border Protection	Host Protection
Attached VBScript HTA	HTTPS	Blocked	Blocked
Attached Tikitorch HTA	HTTPS	Blocked	Blocked
Attached Executable	HTTPS	Blocked	Blocked
Attached Marco Enabled Word Document	HTTPS	Blocked	Blocked
Attached Encrypted Marco Enabled Word Document	HTTPS	Not Blocked	Blocked
Attached OLE-Embedded Word Document	HTTPS	Blocked	Blocked
Attached Encrypted OLE-Embedded Word Document	HTTPS	Not Blocked	Blocked
Attached Encrypted (Velvet Sweatshop) Excel Document	HTTPS	Blocked	Blocked





# Observations

# Overall Observations

- Well configured, maintained, and mature external environment
  - Network security mechanisms routinely blocked testing activities
- Multiple network and email security mechanisms
  - Use of anti-virus (MorphiSec & Windows) identified and prevented the execution all tested payloads
  - Security appliance or service blocked the delivery of all messages containing malicious payloads





# Next Steps

- RPT Team
  - Additional Analysis
  - Draft Report to POC
  
- Dean Lewis
  - Review & validate findings
  - Action Plans to remediate, as appropriate
  - Future work with DHS CISA





Questions?