Agenda

Mangum City Hospital Authority

November 26, 2024 at 5:00 PM

City Administration Building at 130 N Oklahoma Ave.

The Trustees of the Mangum City Hospital Authority will meet in regular session on November 26, 2024, at 5:00 PM, in the City Administration Building at 130 N. Oklahoma Ave, Mangum, OK for such business as shall come before said Trustees.

CALL TO ORDER

ROLL CALL AND DECLARATION OF A QUORUM

CONSENT AGENDA

The following items are considered to be routine and will be enacted by one motion. There will be no separate discussion of these items unless a Board member (or a community member through a Board member) so requests, in which case the item will be removed from the Consent Agenda and considered separately. If any item involves a potential conflict of interest, Board members should so note before adoption of the Consent Agenda.

1. Approve October 22, 2024 regular meeting minutes as present.

2. Approve October 2024 Medical Staff meeting minutes as presented.

3. Approve October 2024 Quality Report.

4. Approve October 2024 Clinic Report.

5. Approve October 2024 CCO Report.

6. Approve October 2024 CEO Report.

7. Approve the following forms, policies, appointments, and procedures previously approved, on 11/14/2024 Quality Committee and on 11/21/2024 Medical Staff.

   Discussion and Possible Action to Approve the Policy and Procedure:MRMC-340B Drug Discount Purchasing Program.

   Discussion and Possible Action to Approve the Policy and Procedure: MRMC-Compliance Manual with Table of Contents attached.

   Discussion related to HIM Delinquencies-none to report.

FURTHER DISCUSSION

REMARKS

Remarks or inquiries by the audience not pertaining to any item on the agenda.

REPORTS

8. Financial Report for October 2024.

OTHER ITEMS

9. Discussion and Possible Action to Approve the Service of Cybersecurity and Infrastructure Security Agency (CISA) for assessment and tabletop services of cybersecurity

10. Discussion and Possible Action to Approve the eClinicalWorks work order for the interface between eClinicalWorks and TruBridge for the Mangum Clinic.

11. Discussion and Possible Action to Approve the TruBridge eClinicalWorks Bidirectional performance interface agreement.

12. Discussion and Possible Action to Approve the TruBridge and eClinicalWorks interface performance expectations agreement.

13. Discussion and Possible Action to Approve the CareLearning-Third Party Content Usage Agreement for the education platform used by the hospital.

14. Discussion and Possible Action to Approve the Tecumseh Oxygen & Medical Supply Agreement for the Provision & Maintenance of Durable Medical Equipment and Business Associate Agreement.

15. Discussion and Possible Action to Approve the Business Associate Agreement Between Mangum Regional Medical Center and Sinor EMS for transport services to and from the hospital.

16. Discussion and Possible Action to Approve ACH authorization form for current vendor Nuance Communications due to changes in their payment policies.

17. Discussion and Possible Action on why payroll checks are being processed a year or more late.

EXECUTIVE SESSION

18. Discuss and make possible action to enter into executive session for the review and approval of **medical staff privileges/credentials/contracts** for the following providers pursuant to 25 O.S. § 307(B)(1):

OPEN SESSION

19. Discussion and possible action with regard to executive session.

STAFF AND BOARD REMARKS
Remarks or inquiries by the governing body members, City Manager, City Attorney or City Employees

NEW BUSINESS
Discussion and possible action on any new business which has arisen since the posting of the Agenda that could not have been reasonably foreseen prior to the time of the posting (25 O.S. 311-10)

ADJOURN
Motion to Adjourn

Duly filed and posted at **5:00 p.m. on the 22nd day of November 2024**, by the Secretary of the Mangum City Hospital Authority.

____
Codi Gutierrez, Secretary

Minutes

Mangum City Hospital Authority Session

October 22, 2024 at 5:00 PM

City Administration Building at 130 N Oklahoma Ave.

The Trustees of the Mangum City Hospital Authority will meet in regular session on October 22, 2024, at 5:00 PM, in the City Administration Building at 130 N. Oklahoma Ave, Mangum, OK for such business as shall come before said Trustees.

CALL TO ORDER

Chairman Vanzant called the meeting to order at 5:01pm.

ROLL CALL AND DECLARATION OF A QUORUM

PRESENT

Trustee Michelle Ford

Trustee Carson Vanzant

Trustee Lisa Hopper

Trustee Ronnie Webb

ABSENT

Trustee Cheryl Lively

ALSO PRESENT

City Attorney Corry Kendall

CONSENT AGENDA

The following items are considered to be routine and will be enacted by one motion. There will be no separate discussion of these items unless a Board member (or a community member through a Board member) so requests, in which case the item will be removed from the Consent Agenda and considered separately. If any item involves a potential conflict of interest, Board members should so note before adoption of the Consent Agenda.

1. Approve September 24, 2024 regular meeting minutes as presented.
2. Approve September 2024 Medical Staff meeting minutes as presented.
3. Approve September 2024 Quality Report.
4. Approve September 2024 Clinic Report.
5. Approve September 2024 CCO Report.
6. Approve September 2024 CEO Report.
7. Approve the following forms, policies, appointments, and procedures previously approved, on 10/10/2024 Quality Committee and on 10/17/2024 Medical Staff.

Discussion and Possible Action to Approve the Policy and Procedure: MRMC-Respiratory Therapy Decannulation Risk Assessment.

Discussion and Possible Action to Approve the Policy and Procedure: MRMC-Decannulation Prevention Program

Discussion and Possible Action to Approve the Policy and Procedure: MRMC- Post Decannulation Analysis Worksheet.

Discussion and Possible Action to Approve the Policy and Procedure: MRMC-Decannulation Precautions

Discussion related to HIM Delinquencies-none to report.

Motion to approve consent items 1, 2, 4, 5, and 6.

Motion made by Trustee Vanzant, Seconded by Trustee Webb.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

FURTHER DISCUSSION

Item 3 - Hopper asked about the issues in the lab because there have been issues over the last couple of months and do they know what the issues are. Martinez explained some of the issues with the interface and new reference lab, CPL. They are hoping to hear about the interface this week so that the issues will be resolved in the reports and correct responses will start coming in through the system. The specimens were rejected due to lack of specimens received. Hopper asked if the hospital's case management was on or off sight, she was concerned they may have missed some services. Martinez explained they have both on and off sight. He explained that part of the readmits may have been because they needed a higher level of care and then they were readmitted. He also stated that they did have some readmits but that was because they went home too early and had to come back but none of them went home without services. Hopper asked about radiology not reading because they were busy and stated that is not an acceptable excuse for a contractor. Martinez explained DIA is very busy and sometimes the hospital does routine readings as STAT read. In this instance they missed their one-hour turnaround and when they were called on it they explained that the test wasn't as critical as a stroke CT. He explained this is being monitored but if they cancel DIA there are very limited resources available. Ford asked about the falls that were reported and if there were 5 different people. Martinez explained three were one patient and the other two falls were two separate patients.

Motion to approve item #3.

Motion made by Trustee Vanzant, Seconded by Trustee Ford.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

Item 7 - No questions.

Motion to approve item #7.

Motion made by Trustee Vanzant, Seconded by Trustee Hopper.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

REMARKS

Remarks or inquiries by the audience not pertaining to any item on the agenda.

None.

REPORTS

8. Financial Report for September 2024.

Financial Report given by Adrian Brownen.

September 2024 Financial Statement Overview

• Statistics

o The average daily census (ADC) for September 2024 was 6.58 – (Year- To-Date 10.87 PY fiscal year end of 11.47).

o Year-To-Date Acute payer mix was approximately 76% MCR/MCR Managed Care combined.

o Year-To-Date Swing Bed payer mix was 87% MCR & 12% MCR Managed Care. For the prior year end those percentages were 90% & 10%, respectively.

• Balance Sheet Highlights

o The cash balance as of September 30, 2024, inclusive of both operating & reserves, was $522K. This a decrease of $140K from August 31, 2024, balance was primarily due to an increase in disbursements.

o Days cash on hand, inclusive of reserves, was 12.1 based on September expenses.

o Net AR decreased by $166K from August.

o Payments of approximately $1.32M were made on AP (prior 3-month avg was $1.65M).

o Cash receipts were $906K less than in the previous month ($1.18M vs $2.09M).

o The Medicare principal balance was completely paid off in the month of August.

• Income Statement Highlights

o Net patient revenue for September 2024 was $1.40M, which is approximately a decrease of $40K from the prior month.

o Operating expenses, exclusive of interest & depreciation, were $1.34M.

o 340B revenue was $19K in September, an increase of $6K from the prior month. YTD revenue was $143K. Net profit from this service line YTD is $33K.

• Clinic (RHC) Income Statement Highlights - actual & projected (includes swing bed rounding):

o Current month average visits per day = 6.43

o Projected operating revenues (YTD) = $414K

o Projected operating expenses (YTD) = $839K

o Projected operating loss (YTD) = -($425K)

Vanzant asked if there was a balance sheet that was available. Boyd explained there is a balance sheet in the packet and that he would go over it. Cash on hand is over 12 days and all Medicare debt has been paid off and they try to maintain at least 10 days on hand. They have a Medicare receivable out and they are expecting that very soon. They are expecting this year's to be around $340,000. Ford asked Boyd to explain the Cohesive loan of $5 million and the accounts payable due to Cohesive of $13 million. Boyd explained that they could not physically pay 9.8 million and pay Cohesive AP so they issued an interest free 0% interest loan for the amount to pay off all the Medicare debt. The AP is mostly payroll and some management fees. Ford asked if they are reserving the cash and using the excess cash to pay off Medicare. Kendall tried to explain it by stating, when it comes to putting debt on the cost report it must be realized at some point. If you don't realize it then it was a false claim and you have to take it off which would mess up the cost report. By reducing the amount of money in a loan it made the debt legitimate thereby allowing us to keep the cost report to allow for credit. Boyd stated that the plan is to try to continuously make significant payments. He added that looking at the aging report from last month, there are a couple of things to write off that were taken care of in the settlement. The only vendors that were owed were 60 days and 90days was for Cohesive. They have tried to make sure all vendors are kept current. The main priority is to make sure the Medicare debt is paid off and to take care of the vendors.

OTHER ITEMS

9. Discussion and possible action with regard to the operations of Mangum Regional Medical Center to include Mangum City Hospital Authority Board, City Commission Board, Hospital Administrator, Cohesive Financial Services and Cohesive CEO.

   Tabled

10. Discussion and Possible Action to Approve The Sysmex Service Agreement Quote for Beyond Care Remote services for Hematology.

    This is a renewal service agreement on the Sysmex machine in the lab. The amount is now $6,462 per year which is down from $8,400 with no changes in the agreement.

    Motion to approve the contract.

    Motion made by Trustee Vanzant, Seconded by Trustee Ford.
    Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

11. Discussion and Possible Action to Approve The Werfen Capital Purchase Proposal to Purchase the Hemochron Signature Elite equipment and services to be used exclusively by the laboratory for coagulation studies.

    Martinez explained this is to perform the coags in the hospital. They are currently doing them on the big chemistry machine. The cost on the big machine is $14,000 per year and the new one will be $9,218 with $668 for supplies. This will include a 2-year service agreement and they do get reimbursed for it. Pricing is guaranteed for 3 years.

    Motion to approve.

    Motion made by Trustee Webb, Seconded by Trustee Vanzant.
    Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

12. Discussion and Possible Action to Approve The Business Associate Agreement Between Mangum Regional Medical Center and ETC Transport to provide EMS transport services to and from the hospital.

    Martinez explained this is part of the condition participation saying they have to have contracts with all vendors and transport agencies are now considered vendors. The Business Association Agreement is to cover HIPPA. They do not have to use this company exclusively and they will use them mostly for non-emergency transport and emergent when Greer County EMS or Survival Flight are not available.

    Motion to approve.

    Motion made by Trustee Hopper, Seconded by Trustee Webb.
    Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

13. Discussion and Possible Action to Approve The Business Associate Agreement Between Mangum Regional Medical Center and Sinor EMS to provide EMS transport services to and from the hospital.

14. Discussion and Possible Action to Approve The Business Associate Agreement Between Mangum Regional Medical and Cross County EMS to provide EMS transport services to and from the hospital.

Martinez explained this is the same situation as item #12.

Motion to approve.

Motion made by Trustee Vanzant, Seconded by Trustee Hopper.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

15. Discussion and Possible Action to Approve The Business Associate Agreement Between Mangum Regional Medical and LifeCare Mobility Transportation to provide EMS transport services to and from the hospital.

Martinez explained this is the same situation as item #12.

Motion to approve.

Motion made by Trustee Webb, Seconded by Trustee Hopper.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

16. Discussion and Possible Action to Approve The ASD Healthcare-Specialty Pharmaceutical Purchase and Sale Agreement for pharmaceutical plasma/specialty product.

Martinez explained this is one of the vendors that works with Amerisource Bergen and they can purchase supplies from them. This will guarantee their GOP pricing.

Motion to approve the sales agreement.

Motion made by Trustee Webb, Seconded by Trustee Hopper.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

17. Discussion and Possible Action to Approve The Russell Electric and Security Services-Quote for wireless panic buttons.

Martinez explained they have Russell's Security for the fire monitoring already and they had the Sheriff's Department come out and check for vulnerabilities at the hospital. They recommended panic buttons for the nurses and the registration windows. With this, there would be three wireless buttons for the charge nurse, ER nurse and another person. There will also be three stationary buttons located at the front registration desk, back registration desk and possibly in Physical Therapy. This initial cost is $895.00 and then $35.00 per month for 3 years. Russell's will monitor and send directly to the Sherriff's Department.

Motion to approve.

Motion made by Trustee Vanzant, Seconded by Trustee Ford.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper
Voting Nay: Trustee Webb

18. Discussion and Possible Action to approve Resolution No. 10-22-2024 adopting a Title VI Plan for the Mangum Regional Medical Center and confirming that the governing body for the Mangum Regional Medical Center Reviewed and Approved the Title VI Plan

    Martinez explained this was an ODOT recommendation after they sent them the minutes from when the board approved the plan. This was not specific enough for them, so a resolution was created. The minutes did not specifically say the board approved the Title VI plan.

    Motion to approve Resolution 10-22-2024 adopting the Title VI plan.

    Motion made by Trustee Webb, Seconded by Trustee Hopper.
    Voting Yea: Trustee Ford, Trustee Hopper, Trustee Webb
    Voting Nay: Trustee Vanzant

STAFF AND BOARD REMARKS
Remarks or inquiries by the governing body members, City Manager, City Attorney or City Employees

Hopper stated that she noticed there were 16 no shows at the clinic and wanted to know if anything had been put in place for reminders to patients. Martinez explained that there were phone calls made by staff the day before to confirm appointments, patients confirmed but did not show. Vanzant inquired about text messages. Martinez explained there is a part of ECW that will do that, but it is $.55 per text message but it will go down the more they send. He stated that as the numbers get greater, they do expect to move toward the automated calls.

Webb asked when the social media would be launched. Martinez stated that they had a meeting last week and they have to get with Legal for the picture release forms. Also, Dr. Sanda and Dr. Nelson are going to start posting on Facebook.

Ford asked if they had any idea why September was so low in the hospital. Martinez stated the referrals from different parts of the state were down. Swing beds are also up and down for other hospitals as well and Medicare is now wanting everyone to be outpatient procedures unless they have underlying issues.

NEW BUSINESS
Discussion and possible action on any new business which has arisen since the posting of the Agenda that could not have been reasonably foreseen prior to the time of the posting (25 O.S. 311-10)

None.

ADJOURN
Motion to Adjourn

Motion made by Trustee Vanzant, Seconded by Trustee Hopper.
Voting Yea: Trustee Ford, Trustee Vanzant, Trustee Hopper, Trustee Webb

Meeting adjourned at 5:45pm.

Carson Vanzant, Chairman

Codi Gutierrez, City Clerk

Mangum Regional Medical Center
Medical Staff Meeting
Thursday
October 17, 2024

MEMBERS PRESENT:

John Chiaffitelli, DO, Medical Director
Laura Gilmore, MD
Sonja Langley, MD
Absent:
Guest:

ALLIED HEALTH PROVIDER PRESENT:

David Arles, APRN-CNP
Mary Barnes, APRN-CNP

NON-MEMBERS PRESENT:

Kelley Martinez, RN, CEO
Chelsea Church, PharmD
Nick Walker, RN, CCO
Meghan Smith, RN, Infection Preventionist
Denise Jackson, RN, Quality
Chasity Howell, RN – Utilization Review
Lynda James, LPN, Pharmacy Tech

1. Call to order
    a. The meeting was called to order at 12:49 pm by Dr. John Chiaffitelli, Medical Director.

2. Acceptance of minutes
    a. The minutes of the September 19, 2024, Medical Staff Meeting were reviewed.
        i. **Action:** Dr. Chiaffitelli, Medical Director, made a motion to approve the minutes.

3. Unfinished Business
    a. None.

.

4. Report from the Chief Executive Officer
    a. Sports physicals continue to take place at our clinic until mid-September.

        ○ Operations Overview
            ○ Patient rounds continue to provide positive feedback from our patients.

- Looking at clinic collections for September we collected a total of $2,066.18 down from $2,493.17 at time of service.
- In the Month of September the hospital collected $19,856.91 total patient payments of which $1,169.88 was upfront collections.
- Our Outpatient Physical Therapy Department has moved to a larger space in the Annex to provide better care for our patients.
- We continue to move forward on the roof we are looking to submit a claim soon.
- We have recently filled two of the four house supervisor positions with local applicants.
  We continue to look for two-night shift house supervisors.
- We are going to be adding a PRN – MD to our Emergency Department rotation, start date is going to be in November.
- We are continuing to look for a Licensed Professional Counselor to head our Strong Minds program.
- Our clinic continues to see new patients every month and welcomes walk-ins.

Written report remains in the minutes.

5. Committee / Departmental Reports

a. Medical Records – August Report

1. There were several things missing from two different acute charts.
The acute charts have been completed.

1.September Report
We are making a decision whether the Swing Bed visits still need to have d/c instructions.

b. Nursing

Patient Care

- MRMC Education included:
  1. Nursing documentation/updates are communicated to nursing staff weekly.
  2. IP sent out notification/education regarding an increase in pertussis.
- MRMC Emergency Department reports 0 patients Left Without Being Seen (LWBS).
- MRMC Laboratory reports 0 contaminated blood culture set(s).
- MRMC Infection Prevention reports 0 CAUTI.
- MRMC Infection Prevention report 0 CLABSI.
- MRMC Infection Prevention reports 0 HAI, or 0 MDRO for the month of September.

Client Service

- Total Patient Days decreased with 214 patient days in September 2024 as compared to 343 patient days in August 2024. This represents an average daily census of 7. In addition, MRMC Emergency Department provided care to 143 patients in September 2024.
- MRMC Case Management reports 22 Total Admissions for the month of September 2024.
- September 2024 COVID-19 Statistics at MRMC: Swabs (0 PCR & 43 Antigen) with 9 Positive.

Preserve Rural Jobs

- The Skills Fair is scheduled for October 23/24.
- MRMC has hired two "core" RN-House Supervisor positions and will hire and additional three more. We have one CNA position open currently. We are still looking to hire an LPN to help in the pharmacy and some on the floow.
- Patients continue to voice their praise and appreciation for the care received at MRMC. We continue to strive for excellence and improving patient/community relations.

Written report remains in minutes.

c. Infection Control

- Old Business
  - a None
- New Business
  - a. N/A
- Data:
  - a, N/A
- Policy & Procedures Review:
  - a. N/A
- Education/In Services
  - a. Monthly EPIC meeting for IP education.
  - b. Weekly Call with Corp. IP.
  - c. Weekly Lunch and Learns.
  - d. Staff education
- Updates: Employees are offered flu shots through the influenza vaccine program. Three annual Fit test completed.
- Annual Items:
  - a. Completed March 2023
  - b. ICRA approved by Board March, 2024.
  - c. 1 ICRA for July 2024

Written report remains in the minutes.

d. Environment of Care and Safety Report

i. Evaluation and Approval of Annual Plans –

i.i. Old Business - -

a. Chrome pipe needs cleaned and escutcheons replaced on hopper in ER – could not replace escutcheons due to corroded piping in wall – capped off leaking pipe under the floor to stop leak – hopper will be covered – remodel postponed.

b. ER Provider office flooring needing replaced. Tile is onsite.- remodel is postponed.

c. EOC, and Life Safety Plans will be evaluated and approved in the October EOC meeting.

i.i.i. New Business

a. Retire EOC Plans:

Retired – LS-301, LS-302, LS-303, LS-304 and LS-305

Written report remains in minutes.

e. Laboratory

i. Tissue Report – None – September, 2024 – Approved

i.i. Transfusion Report – None – September, 2024 – Approved

Written report remains in minutes.

f. Radiology

i. There was a total of – 189 X-Rays/CT/US

i.i. Nothing up for approval

i.i.i. Updates:

- No Updates.

Written report remains in minutes.

g. Pharmacy

i. Verbal Report by PharmD.

i.i. P & T Committee Meeting –
The next P&T Committee Meeting will be held in December, 2024.

i.i.i. Sterile Cipro IV and Levaquin 750mh IV has been added to the shortage list.

Written report remains in the minutes.

h. Physical Therapy

i. No report.

i. Emergency Department

i. No report

j. Quality Assessment Performance Improvement

- Risk Management
  - Grievance – 0
  - Fall with no injury – 3
  - Fall with minor injury – 2
  - Fall with major injury – 0
  - Death – 1
  - AMA/LWBS – 3

- Quality
  - Quality Minutes

- HIM – H&P – Completion – 94%
  Progress Note completion – 100%
- Med event – 3
- After hours access was – 77
- Compliance

Written reports remain in the minutes.

k. Utilization Review

i. Total Patient days for August: 343
i.i. Total Medicare days for August: 287
i.i.i. Total Medicaid days for August: 0
iv. Total Swing Bed days for August: 298
v. Total Medicare SB days for August: 264

Written report remains in the Minutes.

Motion made by Dr. John Chiaffitelli, Medical Director to approve Committee Reports for September, 2024.

6. New Business

a. Review & Consideration of Approval of Policy & Procedures: MRMC – Respiratory Therapy Decannulation Risk Assessment

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Respiratory Therapy Decannulation Risk Assessment.

b.Review & Consideration of Approval of Policy & Procedure: : MRMC – Decannulation Prevention Program

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Decannulation Prevention Program.

c.Review & Consideration of Approval of Policy & Procedure: MRMC – Post Decannulation Analysis Worksheet

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Post Decannulation Analysis Worksheet.

d.Review & Consideration of Approval of a Precautions Sign: MRMC – Decannulation Precautions Sign

i.Motion: made by John Chiaffitelli, DO, Medical Director, to approve MRMC – Decannulation Precautions Sign.

7. Adjourn

a. Dr Chiaffitelli made a motion to adjourn the meeting at 1:11 pm.

Medical Director/Chief of Staff Date

Mangum Regional Medical Center
Quality and Patient Safety Committee Meeting
Agenda for Oct 2024 and Meeting Minutes for Oct 2024

Meeting Location: OR	**Reporting Period: Sept 2024**	
Chairperson: Dr Gilmore	**Meeting Date: 10/10/24**	**Meeting Time: 14:00**
Medical Representative: Dr Gilmore	**Actual Start Time: 1403**	**Actual Finish Time: 1452**
Hospital Administrator/CEO: Kelley Martinez	**Next Meeting Date/Time: 11/14/2024 @ 14:00**	

Mission: To provide our Mangum community and surrounding counties with convenient, gold-standard "dependable and repeatable" patient care, while assisting and supporting all their medical healthcare needs.

**** Items in blue italics denote an item requiring a vote***

I. CALL TO ORDER

Agenda Item	Presenter	Time Allotted	Discussion/Conclusions	Decision/Action Items
A. Call to Order	QM	**1 min**	Called to order at 1403	Approval: First –Tonya, Second – Brittany

II. COMMITTEE MEETING REPORTS & APPROVAL OF MINUTES

Agenda Item	Presenter	Time Allotted	Discussion/Conclusions	Decision/Action Items
A. Quality and Patient Safety Committee 1. ***Approval of Meeting Minutes***	Denise Jackson	**2 min**	Meeting minutes - Sept 2024	Approval: First – Kelley, Second – Nick
B. Environment of Care (EOC) Committee 1. ***Approval of Meeting Minutes***	Mark Chapman	**2 min**	Meeting minutes – Sept 2024	Approval: First – Kelley, Second – Meghan
C. Infection Control Committee 1. ***Approval of Meeting Minutes***	Meghan Smith	**2 min**	Meeting minutes – Sept 2024	Approval; First – Nick, Second - Chasity
D. Pharmacy & Therapeutics (P&T) Committee 1. ***Approval of Meeting Minutes***	Chelsea Church/ Lynda James	**2 min**	Next Meeting – Dec 2024	
E. Heath Information Management (HIM)/Credentialing Committee 1. ***Approval of Meeting Minutes***	Jennifer Dryer/ Kaye Hamilton	**2 min**	Meeting minutes – Aug/Sept 2024	Approval: First – Danielle, Second – Meghan
D. Utilization Review (UR) Committee 1. ***Approval of Meeting Minutes***	Chasity Howell	**2 min**	Meeting minutes – Sept 2024	Approval; First – Jennifer , Second – Brittany

Mangum Regional Medical Center
Quality and Patient Safety Committee Meeting
Agenda for Oct 2024 and Meeting Minutes for Oct 2024

III. DEPARTMENT REPORTS				
Agenda Item	**Presenter**	**Time Allotted**	**Discussion/Conclusions**	**Decision/Action Items**
A. Nursing/Emergency Department	Nick Walker	**5 min**	0 restraints 0 PRBC with no reactions 1 code blue; successful resuscitation with pt transferred to higher level of care for further dx and tx	
B. Radiology	Pam Esparza	**2 min**	2 films repeated; clipped anatomy/patient motion, films repeated with no further issues	
C. Laboratory	Tonya Bowan	**8 min**	2 rejected labs; due to not enough specimen. Dimension – multiple issues requiring service engineer visits for correction Battery in blood bank replaced, during the down time temps were checked daily 1 Lipase was not diluted, this was corrected and re-ran	Director provided training on machine daily monitoring for all techs
D. Respiratory Care	Heather Larson	**2 min**	16 neb changes for the month 0 vent days	
E. Therapy	Chrissy Smith	**2 min**	Pt with assistive needs – 14 Total sessions for the month; 97 -PT 70-OT 0-ST Improved Standard Assessment Scores: 5- PT	

			6- OT 0- ST	
F. Materials Management	Brittany Gray	**2 min**	1 back orders, 0 late orders, 0 recalls	MM workbook not working however issues have been fixed by IT
G. Business Office	Danille Cooper	**2 min**	3 visits in the ED where ID/INS was not obtained nor was a note written by admitting nurse, noted trend with nurse	BOM to maintain log of shift and nurse for these incidents and report findings to CNO/QM
H. Human Resources	Bethany Moore	**2 min**	7 background checks completed for new employees this month All certifications renewed	
I. Environmental Services	Mark Chapman	**2 min**	100% terminal room cleans	
J. Facility/Plant Operations	Mark Chapman	**2 min**	24 extinguishers checked boiler turned off for warm weather months on 4/30/24; no inspections while boiler is not running 1 generator/transfer switch inspection	
K. Dietary	Treva Derr	**2 min**	100% on all logs for the month	
L. Information Technology	Tim Hopen	**2 min**	Data reviewed	CEO to meet with Corporate IT to review workbook data
IV. OLD BUSINESS				
V. NEW BUSINESS				
Agenda Item	**Presenter**	**Time Allotted**	**Discussion/Conclusions**	**Decision/Action Items**
A. New Business	QM	2 min	See Policy Information Below	
VI. QUALITY ASSURANCE/PERFORMANCE IMPROVEMENT DASHBOARD REPORT				
Agenda Item	**Presenter**	**Time Allotted**	**Discussion/Conclusions**	**Decision/Action Items**

A. Volume & Utilization	CM	**5 min**	AMA - 2 inpt/ 2 ER 1-2 inpt; Both patients were assigned dietary restrictions based on admitting dx, frustrations with diet were expressed and demanded to leave. Due to dx, diet was not able to be changed as part of standards of care. Both signed out AMA, all risks/benefits were discussed prior to signing out AMA 1 ER – 1 pt requesting specialty DME, attempts to find supporting dx/medical visits to support need for DME were being made when patient expressed, they were tired of waiting and left without signing AMA. No urgent/emergent medical issues were noted or expressed during this visit 2 ER – Pt to ER for c/o, all testing/assessments were preformed based on patient needs at time of visit, pt expressed desire to leave. Education provided on waiting for test results however pt continued to express desire to leave, discussed R/B and signed out AMA. Test results were later called to patient and need to return for further treatment expressed, pt later returned for further treatment	
B. Case Management	CM	**8 min**	0 re-admits for the month	

C. Risk Management	QM	**10 min**	0 complaint 1 grievance – Pt reported inappropriate conversation that took place with pt/staff Falls – 1 fall with minor injury; pt found on floor with redness to head, shoulder, hip. No other injuries noted, fall precautions put in place as appropriate for patient Mortality - 1 SWB, anticipated due to dx process	Grievance – CEO met with local/corporate HR and staff member to discuss reported grievance; no supportive findings noted during investigation
D. Nursing	CCO	**2 min**	2 IV admiration follow ups not completed	Charge nurses/ER nurses continue to be educated on following up on IV reassessments
E. Emergency Department	CCO/QM	**5 min**	ER readmits - 6 1.) Pt presented with initial c/o treated and d/c. Returned later with same c/o and found to be non-compliant with meds. 2.) Pt present with initial c/o, treated and d/c. Returned later with same c/o, additional testing preformed with additional dx added and treatment prescribed, pt d/c. Pt returned with on-going c/o; education on dx and continuation of tx as ordered	

			3.) Pt presented with initial c/o, treated and dc. Returned later with different c/o, pt evaluation noted need for surgical intervention, pt transferred for higher level of care 4.) Pt presented with initial c/o, treated and dc. Returned later with continued c/o, additional tx added with PCP f/u recommended. 5.) Pt presented with initial c/o, all testing/assessments were performed based on patient needs at time of visit, pt expressed desire to leave. Education provided on waiting for test results however pt continued to express desire to leave, discussed R/B and signed out AMA. Test results were later called to patient and need to return for further treatment expressed, pt later returned for further treatment	
F. Pharmacy & Therapeutics (P&T)	Pharmacy	**2 min**	Next P&T – Dec 2024 After hours access - 57 ADR - 0 Med errors – 0	
G. Respiratory Care	RT	**2 min**	100% on chart checks	
H. Wound Care	WC	**2 min**	1 for reporting period – Pt high risk for breakdown, developed wound after 30+	Wound Care spoke with nursing on importance of positioning for wound

			hospital days. Wound care ordered with dressings, air mattress and positioning.	healing with additional wound care education during skills fair this month
I. Radiology	RAD	**2 min**	2 - delays in reads for the month (1 CT/ 1 Xray)	Rad staff remains in contact with DIA regarding delays and ETA on reads
J. Laboratory	LAB	**5 min**	No blood culture contaminations	
K. Infection Control/Employee Health	IC/EH	**5 min**	No HAIs for the reporting period	
L. Health Information Management (HIM)	HIM	**2 min**	Aug – clarification was done on the suture visits for MR/Billing Sept – Several issues with "attending provider" on charts, this is being corrected on the effected charts and discussion have occurred to prevent any further issues. Providers can no longer use SOAP notes, education has been provided.	
M. Dietary	Dietary	**2 min**	100 % on all logs with no other issues at this time	
N. Therapy	Therapy	**2 min**	Outpatient remains steady, no speech therapy needs this reporting period	
O. Human Resources (HR)	HR	**2 min**	90-day competency - None Due Annual education – 1 PT PRN	Discussed PT with continued education needs, HR/CEO will follow up on next steps with employee
P. Business Office	BOM	**2 min**	5 OP visits missed on cost share, BOM noted trend	BOM provided education with staff member on correct cost share collections
Q. Environmental Services	EVS	**2 min**	10/10 on room cleans	
R. Materials Management	MM	**2 min**	Requisitions – going well for all depts	HIM is not able to complete requisitions at this time, working on fix for this
S. Life Safety	PO	**2 min**	100%	
T. Emergency Preparedness	EP	**2 min**	5 employee oriented	

U. Information Technology	IT	**2 min**	Data reviewed	
V. Outpatient Services	Therapy	**2 min**	Data tool being added to workbook	Email out to creator regarding this still not on workbook
W. Strong Minds	N/A	N/A	N/A	Policies were approved in April 2024 for the SM program, looking for Councilor?
VII. POLICIES & PROCEDURES				
Agenda Item	**Presenter**	**Time Allotted**	**Discussion/Conclusions**	**Decision/Action Items**
A. Review and ***Approve***	QM	10 min	1. Respiratory Therapy Decannulation Risk Assessment 2. Decannulation Prevention Program 3. Post Decannulation Analysis Worksheet 4. Decannulation Precautions	First approval – Kelley Second approval – Nick
VIII. PERFORMANCE IMPROVEMENT PROJECTS				
IX. OTHER				
X. ADJOURNMENT				
Agenda Item	**Presenter**	**Time Allotted**	**Discussion/Conclusions**	**Decision/Action Items**
A. Adjournment	QM	1 min	There being no further business, meeting adjourned at 1452 by Brittany seconded by Chasity	

Mangum Regional Medical Center
Quality and Patient Safety Committee Meeting
Agenda for Oct 2024 and Meeting Minutes for Oct 2024

MEMBERS & INVITED GUESTS				
Voting MEMBERS				
Kelley Martinez	Nick Walker	Carlos Mendoza	Lynda James	Treva Derr
Chasity Howell	Jennifer Dreyer	Danielle Cooper	Meghan Smith	Pam Esparza
Brittany Gray	Tonya Bowen	Bethany Moore	Kaye Hamilton (teams)	Dr G (teams)
Dianne (teams)		□	□	□
Non-Voting MEMBERS				
Denise Jackson	□	□	□	□

Item 4.

Clinic Operations Report

Mangum Family Clinic

October 2024

Monthly Stats	October 23	October 24
Total Visits	192	202
Provider Prod	127	183
RHC Visits	180	196
Nurse Visits	2	6
Televisit	0	0
Swingbed	10	4

Provider Numbers	RHC	TH	SB
Ogembo	168		
Chiaffitelli			4
Sanda	28		
other			

Payor Mix	
Medicare	59
Medicaid	63
Self	9
Private	71

Visits per Geography	
Mangum	171
Granite	15
Altus	4
Duke	1

Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Visits	167	123	164	166	164	127	148	198	192	202			

Clinic Operations:

- First Credentialing is working on Dr. Sanda credentialling issue.
- Leslie Desmet is working with eCW on a formal cost report for a lab interface between Trubridge and eCW.

Quality Report:

Improvement Measure	Actual	Goal	Comments
Reg Deficiencies	0	0	10 audited, No deficiencies
Patient Satisfaction	31	5	24 excellent; 7 good
New Patients	30	10	Good solid numbers
No Show	13.4%	<12%	33
Expired Medications	0	0	None noted.

Outreach:

- Nothing specific to report. Clinic continues to support the community by providing quality compassionate care.

Summary:

- Mangum Clinic is continuing to grow with the help of Dr. Sanda. We have seen an increase in new patients as we saw 30 this month. Expect solid growth in the clinic once Dr. Sanda has been credentialed with all insurances.

"You love, you serve, and you show people you care. It's the simplest, most powerful, greatest, success model of all time." Joe Gordon.

Mangum Regional
Medical Center

Chief Clinical Officer Report
October 2024

Patient Care

- MRMC Education included:
  1. Nursing documentation/updates are communicated to nursing staff weekly.
  2. Skills fair for nursing and RT staff completed 10/23-24!
  3. Pyxis education will begin over the course of the next few weeks.
- MRMC Emergency Department reports that there are 0 patients Left Without Being Seen (LWBS).
- MRMC Laboratory reports 0 contaminated blood culture set(s).
- MRMC Infection Prevention reports 0 CAUTI.
- MRMC Infection Prevention report 0 CLABSI.
- MRMC Infection Prevention reports 0 HAI and 0 MDRO for the month of September.

Client Service

- Total Patient Days increased with 227 patient days in October 2024 as compared to 214 patient days in September 2024. This represents an average daily census of 8. In addition, MRMC Emergency Department provided care to 130 patients in October 2024.
- MRMC Case Management reports 20 Total Admissions for the month of October 2024.
- September 2024 COVID-19 statistics at MRMC: Swabs (0 PCR & 42 Antigen) with 3 Positive.

Mangum Regional Medical Center
Monthly Census Comparison

	Jan	Feb	Mar	April	May	June	July	Aug	Sept	Oct	Nov	Dec
Inpatient	30	36	25	20	30	34	27	28	22	20		
Swing Bed	10	18	10	10	12	19	14	12	6	9		
Observation	3	1	2	2	2	0	3	0	0	1		
Emergency Room	175	182	131	125	144	142	132	144	143	130		
Lab Completed	2377	2439	2004	1832	1961	1982	1987	2103	1895	2019		
Rad Completed	128	199	151	182	165	160	143	199	189	170		
Ventilator Days	0	0	0	0	0	0	0	0	0	0		

Preserve Rural Jobs and Culture Development

- MRMC has hired two “core” RN-House Supervisor positions and will hire an additional three more. We have one CNA position open currently.
- Patients continue to voice their praise and appreciation for the care received at MRMC. We continue to strive for excellence and improving patient/community relations.

Mangum Regional Medical Center

COHESIVE HEALTHCARE MANAGEMENT + CONSULTING

Chief Executive Officer Report
October 2024

Operations Overview

- Patient rounds continue to provide positive feedback from our patients.
- Looking at clinic collections for October we collected a total of $2,477.09 up from $2,066.18 at time of service.
- In the Month of October, the hospital collected $17989.41 total patient payments of which $467.25 was upfront collections.
- We continue to move forward on the roof our public adjuster and the insurance adjuster has been to the facility.
- The PRN MD for the Emergency Department is not going to be starting in November, it looks like he is going to be starting in December.
- Clinic numbers continue to be at the low end due to insurance credentialling with Dr. Sanda he is only able to see Medicare Patients currently.
- We are continuing to look for a Licensed Professional Counselor to head our Strong Minds program.
- We are starting to repair patient rooms. We are repairing walls, paint, and flooring.
- We received notification that our Title VI Grant was approved. We are going to start moving forward with that program.

Mangum Board Meeting Financial Reports
September 30, 2024

	REPORT TITLE
1	Financial Summary (Overview)
2	Cash Receipts - Cash Disbursements - NET
3	Financial Update (page 1)
4	Financial Update (page 2)
5	Stats
6	Balance Sheet Trend
7	Cash Collections Trend
8	Medicare Payables (Receivables)
9	Current Month Income Statement
10	Income Statement Trend
11	RHC YTD Income Statement
12	AP Aging Summary

Item 8.

Mangum Regional Medical Center
Financial Summary
October 31, 2024

	Prior Month	Current Month	**Oct-24** Year-to-Date	**Mthly Avg** Year-to-Date
ADC (Average Daily Census)	**6.80**	**7.26**	**10.50**	**10.50**
Payer Mix % (Acute):				
MCR	38.00%	47.50%	54.02%	
MCR Mgd Care	34.00%	7.50%	22.06%	
All Others	28.00%	45.00%	23.92%	
Total	100.00%	100.00%	100.00%	
Payer Mix % (SWB):				
MCR	94.81%	91.35%	87.71%	
MCR Mgd Care	5.19%	8.65%	11.22%	
All Others	0.00%	0.00%	1.07%	
Total	100.00%	100.00%	100.00%	
Operating margin	76,396	(2,456)	(901,735)	*(90,174)*
Operating Margin (Current Month vs Mthly Avg)	*166,570*	*87,718*		
NPR (Net Patient Revenue)	1,395,383	1,503,915	13,531,411	*1,353,141*
NPR (Current Month vs Mthly Avg)	*42,241*	*150,774*		
Operating Expenses	1,339,867	1,527,596	14,614,312	*1,461,431*
Oper Exp (CM vs Mthly Avg)	*(121,564)*	*66,165*		
NPR % of Oper Exp	**104.1%**	**98.4%**	**92.6%**	
Patient Days	204	225	3,203	*320*
Oper Exp / PPD	$ 6,568	$ 6,789	$ 4,563	
# of Months	**1**	**1**	**10**	
Cash Receipts (rnd)	**1,183,508**	**1,779,690**	**13,398,872**	*1,339,887*
Cash Receipts (CM vs Mthly Avg)	*(156,379)*	*439,803*		
Cash as a % of NPR (s/b 100% min)	**84.8%**	**118.3%**	**99.0%**	
Calendar Days	30	31	305	
Operating Exp / Day	$ 44,662	$ 49,277	$ 47,916	
Cash - (unrestricted)	522,262	1,145,664	1,145,664	
Days Cash-On-Hand	**11.7**	**23.2**	**23.9**	
MCR Rec (Pay) - "as stated - but to be adjusted"	431,712	522,493		
AP & Accrued Liab	15,629,541	16,007,503		
Accounts Receivable (at net)	905,815	783,204		
Per AP aging schedule (incl. accruals)	**Sep-24**	**Oct-24**	Net Change	
Account Payable - Cohesive	13,275,114	13,954,444	679,330	
Account Payable - Other	2,354,427	2,053,059	(301,368)	
Total	15,629,541	16,007,503	377,962	
Cohesive Loan	4,993,698	4,962,681	(31,017)	

Item 8.

Mangum Regional Medical Center
Cash Receipts - Cash Disbursements Summary
10/31/24

	Current Month	COVID	Total Less COVID	Year-To-Date	COVID	Year-To-Date Less COVID
Cash Receipts	$ 1,779,690	$ -	$ 1,779,690	$ 13,398,872	$ -	$ 13,398,872
Cash Disbursements	$ 1,154,658	$ -	$ 1,154,658	$ (3,890,983)	$ -	$ (3,890,983)
NET	$ 2,934,348	$ -	$ 2,934,348	$ 9,507,889	$ -	$ 9,507,889
				-		

	Prior Month	COVID	Total Less COVID	Prior Month YTD	COVID	Prior Month YTD Less COVID
Cash Receipts	$ 1,183,508	$ -	$ 1,183,508	$ 11,619,182	$ -	$ 11,619,182
Cash Disbursements	$ 1,322,228	$ -	$ 1,322,228	$ (5,045,641)	$ -	$ (5,045,641)
NET	$ 2,505,737	$ -	$ 2,505,737	$ 6,573,541	$ -	$ 6,573,541

Nov 26, 2024

Board of Directors
Mangum Regional Medical Center

October 2024 Financial Statement Overview

- Statistics
  - The average daily census (ADC) for October 2024 was **7.26** – (Year-To-Date **10.50** PY fiscal year end of **11.47**).
  - Year-To-Date Acute payer mix was approximately **55%** MCR/MCR Managed Care combined.
  - Year-To-Date Swing Bed payer mix was **91%** MCR & **9%** MCR Managed Care. For the prior year end those percentages were **90% & 10%,** respectively.

- Balance Sheet Highlights
  - The cash balance as of October 31, 2024, inclusive of both operating & reserves, was **$1.15M**. This an increase of **$623K** from September 30, 2024, balance was primarily due to an increase in receipts.
  - Days cash on hand, inclusive of reserves, was **23.2** based on October expenses.
  - Net AR decreased by **$123K** from October.
  - Payments of approximately **$1.15M** were made on AP (prior 3-month avg was **$1.68M**).
  - Cash receipts were **$596K** more than in the previous month **($1.78M vs $1.18M).**
  - The Medicare principal balance was completely paid off in the month of August.

Item 8.

- Income Statement Highlights
  - Net patient revenue for October 2024 was **$1.52M**, which is approximately an increase of **$122K** from the prior month.
  - Operating expenses, exclusive of interest & depreciation, were **$1.53M**.
  - 340B revenue was **$19K** in October, this is consistent with the prior month. YTD revenue was **$163K**. Net profit from this service line YTD is **$36K**.

- Clinic (RHC) Income Statement Highlights - actual & projected (includes swing bed rounding):
  - Current month average visits per day = 6.64
  - Projected operating revenues (YTD) = $418K
  - Projected operating expenses (YTD) = $852K
  - Projected operating loss (YTD) = -($433K)

Item 8.

MANGUM REGIONAL MEDICAL CENTER

Admissions, Discharges & Days of Care

Fiscal Year 2024

											12/31/2024	12/31/2023
	January	**February**	**March**	**April**	**May**	**June**	**July**	**August**	**September**	**October**	**YTD**	**YTD**
Admissions												
Inpatient	19	18	15	10	18	15	13	16	16	11	151	178
Swingbed	10	18	10	10	12	18	14	12	6	9	119	137
Observation	3	1	2	2	2	0	3	0	0	1	14	21
	32	37	27	22	32	33	30	28	22	21	284	336
Discharges												
Inpatient	20	17	12	12	18	17	11	17	15	10	149	178
Swingbed	8	12	8	13	13	14	15	14	8	9	114	132
Observation	3	1	2	2	2	0	3	0	0	1	14	21
	31	30	22	27	33	31	29	31	23	20	277	331
Days of Care												
Inpatient-Medicare	24	38	27	25	29	32	26	23	19	19	262	356
Inpatient-Other	67	15	17	8	20	11	11	22	31	21	223	274
Swingbed-Medicare	102	268	383	311	276	255	235	239	146	169	2,384	3,161
Swingbed-Other	56	31	21	11	15	64	53	59	8	16	334	340
Observation	4	1	3	3	4	0	3	0	0	1	19	21
	253	353	451	358	344	362	328	343	204	226	3,222	4,152
Calendar days	31	29	31	30	31	30	31	31	30	31	305	365
ADC - (incl OBS)	8.16	12.17	14.55	11.93	11.10	12.07	10.58	11.06	6.80	7.29	10.56	11.38
ADC	8.03	12.14	14.45	11.83	10.97	12.07	10.48	11.06	6.80	7.26	10.50	11.32
ER	227	237	145	125	150	140	136	162	143	130	1,595	1,677
Outpatient	106	98	103	127	134	118	137	126	143	159	1,251	1,832
RHC	177	176	148	137	123	140	133	150	139	199	1,522	1,978

MANGUM REGIONAL MEDICAL CENTER

Comparative Balance Sheet - Unaudited
Fiscal Year 2024

	January	February	March	April	May	June	July	August	September	October	12/31/23	Variance
Cash And Cash Equivalents	928,483	646,998	809,154	996,013	1,230,088	966,740	733,502	661,771	522,262	1,145,664	80,298	1,065,367
Reserved Funds	-	-	-	-	-	-	-	-	-	-	812,189	(812,189)
Patient Accounts Receivable, Net	1,029,644	1,482,640	1,457,086	1,296,358	978,809	1,135,593	1,125,516	1,072,047	905,815	783,204	1,410,015	(626,811)
Due From Medicare	300,000	150,000	150,000	150,000	262,000	333,000	650,552	168,391	431,393	522,174	0	522,174
Inventory	255,138	261,348	267,175	265,782	271,231	271,221	266,904	261,798	261,690	261,153	259,367	1,786
Prepaids And Other Assets	1,866,039	1,838,554	1,801,875	1,782,687	1,837,325	1,789,629	1,732,244	1,698,945	1,682,707	1,669,774	1,897,615	(227,841)
Capital Assets, Net	1,829,169	1,799,080	1,768,991	1,738,903	1,708,814	1,678,726	1,651,307	1,621,218	1,591,130	1,572,641	1,859,246	(286,605)
Total Assets	6,208,472	6,178,619	6,254,282	6,229,743	6,288,268	6,174,908	6,160,024	5,484,170	5,394,998	5,954,610	6,318,729	(364,119)
Accounts Payable	13,278,998	13,580,039	13,938,685	13,839,576	14,215,610	14,379,350	14,482,354	14,738,134	14,736,817	15,114,779	12,876,396	2,238,383
AHSO Related AP	892,724	892,724	892,724	892,724	892,724	892,724	892,724	892,724	892,724	892,724	892,724	0
Deferred Revenue	-	-	-	226,129	113,064	-	169,940	127,112	-	226,129	0	226,129
Due To Medicare	2,086,019	1,952,438	1,817,700	1,767,460	1,716,728	1,665,483	1,613,738	(319)	(319)	(319)	2,218,453	(2,218,772)
Covid Grant Funds	-	-	-	-	-	-	-	-	-	-	0	0
Due To Cohesive - PPP Loans	-	-	-	-	-	-	-	-	-	-	0	0
Notes Payable - Cohesive	5,241,832	5,210,815	5,179,799	5,148,782	5,117,765	5,086,748	5,055,732	5,024,715	4,993,698	4,962,681	5,272,849	(310,168)
Notes Payable - Other	30,675	23,247	23,247	23,247	17,948	12,649	7,351	2,052	(3,247)	(8,546)	38,045	(46,590)
Alliantz Line Of Credit	-	-	-	-	-	-	-	-	-	-	0	0
Leases Payable	271,991	271,189	270,384	269,576	269,072	268,257	267,440	266,619	265,794	260,087	272,789	(12,703)
Total Liabilities	21,802,238	21,930,451	22,122,538	22,167,493	22,342,911	22,305,212	22,489,277	21,051,036	20,885,468	21,447,536	21,571,256	(123,720)
Net Assets	(15,593,766)	(15,751,832)	(15,868,256)	(15,937,750)	(16,054,644)	(16,130,304)	(16,329,253)	(15,566,866)	(15,490,470)	(15,492,925)	(15,252,526)	(237,944)
Total Liablities and Net Assets	6,208,472	6,178,619	6,254,282	6,229,743	6,288,268	6,174,908	6,160,024	5,484,170	5,394,998	5,954,610	6,318,729	(361,664)

Item 8.

Mangum Regional Medical Center
Cash Receipts & Disbursements by Month

2022				2023			2024		
		Stimulus							
Month	Receipts	Funds	Disbursements	Month	Receipts	Disbursements	Month	Receipts	Disbursements
Jan-22	2,163,583		1,435,699	Jan-23	1,290,109	1,664,281	Jan-24	1,187,504	1,150,522
Feb-22	1,344,463	254,626	1,285,377	Feb-23	1,506,708	1,809,690	Feb-24	708,816	995,157
Mar-22	789,800		1,756,782	Mar-23	1,915,435	1,109,683	Mar-24	1,236,158	1,073,824
Apr-22	1,042,122		1,244,741	Apr-23	2,005,665	1,365,533	Apr-24	1,645,373	1,483,022
May-22	898,311		1,448,564	May-23	1,436,542	2,237,818	May-24	1,273,007	1,062,762
Jun-22	1,147,564		1,225,070	Jun-23	1,777,525	1,506,459	Jun-24	950,928	1,216,556
Jul-22	892,142		979,914	Jul-23	1,140,141	1,508,702	Jul-24	1,344,607	1,562,407
Aug-22	890,601		1,035,539	Aug-23	1,600,786	1,352,905	Aug-24	2,089,281	2,176,381
Sep-22	2,225,347		1,335,451	Sep-23	1,490,569	1,295,680	Sep-24	1,183,508	1,322,228
Oct-22	1,153,073		1,233,904	Oct-23	1,211,980	1,345,813	Oct-24	1,779,690	1,154,658
Nov-22	935,865		1,476,384	Nov-23	985,475	1,355,224	Nov-24		
Dec-22	1,746,862		1,073,632	Dec-23	929,990	1,191,570	Dec-24		
	15,229,733	254,626	15,531,057		17,290,925	17,743,359		13,398,872	13,197,517
Subtotal FY 2022	15,484,359			Subtotal FY 2023	17,290,925		Subtotal FY 2024	13,398,872	

Mangum Regional Medical Center
Medicare Payables by Year

	Original Balance	Balance as of 10/31/24	Total Interest Paid as of 10/31/24
2016 C/R Settlement	1,397,906.00	-	205,415.96
2017 Interim Rate Review - 1st	723,483.00	-	149,425.59
2017 Interim Rate Review - 2nd	122,295.00	-	20,332.88
2017 6/30/17-C/R Settlement	1,614,760.00	-	7,053.79
2017 12/31/17-C/R Settlement	(535,974.00)	(318.61)	269,191.14
2017 C/R Settlement Overpayment	3,539,982.21	-	-
2018 C/R Settlement	1,870,870.00	-	241,040.31
2019 Interim Rate Review - 1st	323,765.00	-	5,637.03
2019 Interim Rate Review - 2nd	1,802,867.00	-	277,488.75
2019 C/R Settlement	(967,967.00)	-	-
2020 C/R Settlement	(3,145,438.00)	-	-
FY21 MCR pay (rec) estimate	(1,631,036.00)	-	-
FY22 MCR pay (rec) estimate	(318,445.36)	-	-
2016 C/R Audit - Bad Debt Adj	348,895.00	-	16,927.31
2018 MCR pay (rec) Audit est.	(34,322.00)	-	-
2019 MCR pay (rec) Audit est.	(40,612.00)	-	-
2020 MCR pay (rec) Audit	(74,956.00)	-	-
FY23 (8-month IRR) L4315598	95,225.46	-	7,038.71
FY23 (8-month IRR) L4315599	1,918,398.00	-	155,799.09
FY23 MCR pay (rec) remaining estimate	-		-
FY24 MCR pay (rec) estimate	-	(522,174.00)	
Total	**7,009,696.31**	**(522,492.61)**	**1,355,350.56**

Mangum Regional Medical Center
Statement of Revenue and Expense
For The Month and Year To Date Ended October 31, 2024
Unaudited

MTD					YTD			
Actual	Budget	Variance	% Change		Actual	Budget	Variance	% Change
206,471	260,956	(54,486)	-21%	Inpatient revenue	2,872,128	2,576,248	295,880	11%
969,940	1,193,612	(223,672)	-19%	Swing Bed revenue	12,571,870	11,737,188	834,682	7%
614,988	581,409	33,580	6%	Outpatient revenue	6,416,328	5,965,020	451,308	8%
197,507	156,747	40,760	26%	Professional revenue	2,108,328	1,652,659	455,669	28%
1,988,906	2,192,724	(203,818)	-9%	Total patient revenue	23,968,655	21,931,115	2,037,539	9%
675,616	740,135	(64,519)	-9%	Contractual adjustments	12,494,088	7,487,347	5,006,741	67%
(301,931)	-	(301,931)	#DIV/0!	Contractual adjustments: MCR Settlement	(1,249,643)	-	(1,249,643)	#DIV/0!
111,307	79,595	31,712	40%	Bad debts	(807,202)	796,948	(1,604,150)	-201%
484,991	819,729	(334,738)	-41%	Total deductions from revenue	10,437,243	8,284,295	2,152,948	26%
1,503,915	1,372,995	130,920	10%	Net patient revenue	13,531,411	13,646,820	(115,409)	-1%
1,288	3,099	(1,811)	-58%	Other operating revenue	18,503	30,959	(12,456)	-40%
19,937	12,607	7,330	58%	340B REVENUES	162,662	126,069	36,593	29%
1,525,140	1,388,701	136,440	10%	Total operating revenue	13,712,577	13,803,849	(91,272)	-1%
				Expenses				
423,535	400,394	23,141	6%	Salaries and benefits	4,208,964	3,929,650	279,315	7%
69,452	143,994	(74,542)	-52%	Professional Fees	716,819	1,439,945	(723,126)	-50%
489,693	361,146	128,547	36%	Contract labor	4,067,046	3,575,629	491,417	14%
111,174	141,523	(30,349)	-21%	Purchased/Contract services	1,217,426	1,414,679	(197,253)	-14%
225,000	225,000	-	0%	Management expense	2,250,000	2,250,000	-	0%
92,943	97,944	(5,000)	-5%	Supplies expense	871,101	969,408	(98,307)	-10%
19,029	30,300	(11,272)	-37%	Rental expense	221,235	303,004	(81,769)	-27%
12,687	18,358	(5,671)	-31%	Utilities	141,165	183,579	(42,414)	-23%
1,034	1,085	(52)	-5%	Travel & Meals	9,299	10,851	(1,552)	-14%
10,697	12,130	(1,433)	-12%	Repairs and Maintnenance	111,668	121,300	(9,633)	-8%
16,416	11,415	5,001	44%	Insurance expense	113,345	114,148	(803)	-1%
9,000	20,773	(11,773)	-57%	Other Expense	111,258	207,733	(96,475)	-46%
16,734	8,187	8,547	104%	340B EXPENSES	126,222	81,612	44,610	55%
1,497,393	1,472,249	25,144	2%	Total expense	14,165,548	14,601,537	(435,990)	-3%
27,748	(83,548)	111,296	-133%	EBIDA	(452,971)	(797,689)	344,718	-43%
1.8%	-6.0%	7.84%		EBIDA as percent of net revenue	-3.3%	-5.8%	2.48%	
115	23,368	(23,254)	-100%	Interest	147,879	260,807	(112,928)	-43%
30,088	49,698	(19,609)	-39%	Depreciation	300,886	496,979	(196,093)	-39%
(2,456)	(156,615)	154,159	-98%	Operating margin	(901,735)	(1,555,475)	653,739	-42%
-	-	-		Other	-	-	-	
-	-	-		Total other nonoperating income	-	-	-	
(2,456)	(156,615)	154,159	-98%	Excess (Deficiency) of Revenue Over Expenses	(901,735)	(1,555,475)	653,739	-42%
-0.16%	-11.28%	11.12%		Operating Margin %	-6.58%	-11.27%	4.69%	

MANGUM REGIONAL MEDICAL CENTER

Statement of Revenue and Expense Trend - Unaudited

Fiscal Year 2024

	January	February	March	April	May	June	July	August	September	October	YTD
Inpatient revenue	553,917	328,884	236,205	196,935	317,963	253,385	216,458	258,025	303,884	206,471	2,872,128
Swing Bed revenue	691,403	1,305,865	1,741,728	1,452,094	1,461,877	1,563,284	1,319,862	1,282,846	782,971	969,940	12,571,870
Outpatient revenue	745,496	798,546	552,340	675,619	606,736	538,539	588,027	675,787	620,249	614,988	6,416,328
Professional revenue	191,359	268,737	196,841	210,516	214,718	202,400	207,252	221,195	197,804	197,507	2,108,328
Total patient revenue	2,182,175	2,702,032	2,727,115	2,535,164	2,601,295	2,557,609	2,331,600	2,437,852	1,904,908	1,988,906	23,968,655
Contractual adjustments	1,194,669	1,354,471	1,363,095	1,126,715	2,317,722	1,268,964	1,051,072	1,399,239	742,526	675,616	12,494,088
Contractual adjustments: MCR Settlement	(300,000)	150,000	-	-	(112,000)	(71,000)	(317,552)	(34,158)	(263,002)	(301,931)	(1,249,643)
Bad debts	66,677	56,019	13,598	70,776	(866,928)	3,530	70,560	(362,743)	30,001	111,307	(807,202)
Total deductions from revenue	961,346	1,560,491	1,376,693	1,197,491	1,338,794	1,201,494	804,079	1,002,338	509,525	484,991	10,437,243
Net patient revenue	1,220,829	1,141,541	1,350,421	1,337,672	1,262,501	1,356,114	1,527,520	1,435,514	1,395,383	1,503,915	13,531,411
Other operating revenue	2,507	1,439	1,671	3,522	2,606	1,311	1,818	1,008	1,333	1,288	18,503
340B REVENUES	37,399	17,167	14,616	10,643	6,757	8,253	14,880	13,462	19,548	19,937	162,662
Total operating revenue	1,260,735	1,160,148	1,366,708	1,351,837	1,271,864	1,365,678	1,544,218	1,449,984	1,416,263	1,525,140	13,712,577
	84.7%	86.6%	91.1%	94.1%	90.9%	94.1%	87.6%	95.1%	104.1%	98.4%	92.6%
Expenses											
Salaries and benefits	411,278	535,269	472,469	436,412	416,357	359,502	371,155	372,779	410,209	423,535	4,208,964
Professional Fees	158,386	(37,292)	62,832	64,972	36,261	94,261	112,557	65,923	89,469	69,452	716,819
Contract labor	298,317	291,650	364,102	320,557	345,990	390,056	712,751	440,549	413,382	489,693	4,067,046
Purchased/Contract services	91,358	88,301	119,963	141,455	146,479	158,021	126,147	183,984	50,544	111,174	1,217,426
Management expense	225,000	225,000	225,000	225,000	225,000	225,000	225,000	225,000	225,000	225,000	2,250,000
Supplies expense	88,273	75,565	103,550	86,191	101,981	97,324	75,175	103,159	46,941	92,943	871,101
Rental expense	33,505	28,767	26,139	36,564	13,147	18,683	17,006	14,310	14,084	19,029	221,235
Utilities	25,813	15,200	12,810	14,755	10,905	11,211	11,366	11,012	15,408	12,687	141,165
Travel & Meals	-	1,802	1,841	1,106	670	349	1,112	396	989	1,034	9,299
Repairs and Maintnenance	12,246	10,628	10,277	11,356	8,198	9,414	15,646	12,477	10,728	10,697	111,668
Insurance expense	12,672	12,896	12,677	12,749	13,582	8,901	6,102	8,676	8,676	16,416	113,345
Other	10,525	8,288	11,834	11,225	11,611	12,932	12,233	12,346	11,264	9,000	111,258
340B EXPENSES	21,375	11,198	9,880	10,402	10,500	8,124	9,877	15,166	12,968	16,734	126,222
Total expense	1,388,748	1,267,272	1,433,374	1,372,743	1,340,679	1,393,776	1,696,127	1,465,775	1,309,661	1,497,393	14,165,548
EBIDA	$ (128,013)	$ (107,125)	$ (66,665)	$ (20,905)	$ (68,815)	$ (28,098)	$ (151,908)	$ (15,791)	$ 106,602	$ 27,748	$ (452,971)
EBIDA as percent of net revenue	-10.2%	-9.2%	-4.9%	-1.5%	-5.4%	-2.1%	-9.8%	-1.1%	7.5%	1.8%	-3.3%
Interest	22,090	20,853	19,670	18,500	17,990	17,474	16,952	14,117	117	115	147,879
Depreciation	30,089	30,089	30,089	30,089	30,089	30,089	30,089	30,089	30,089	30,088	300,886
Operating margin	$ (180,192)	$ (158,066)	$ (116,424)	$ (69,494)	$ (116,893)	$ (75,660)	$ (198,949)	$ (59,997)	$ 76,396	$ (2,456)	$ (901,735)
Other	-	-	-	-	-	-	-	-	-	-	-
Total other nonoperating income	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Excess (Deficiency) of Revenue Over Expenses	(180,192)	(158,066)	(116,424)	(69,494)	(116,893)	(75,660)	(198,949)	(59,997)	76,396	(2,456)	(901,735)
Operating Margin % (excluding other misc. reve	-14.29%	-13.62%	-8.52%	-5.14%	-9.19%	-5.54%	-12.88%	-4.14%	5.39%	-0.16%	-6.58%

Item 8.

	10/31/2024		"Annualized"
On-Site Visits -->	1,448	**On-Site Visits -->**	1,738
On-Site Visit / Bus Day -->	6.64	**On-Site Visit / Bus Day -->**	6.71

Mangum Family Clinic

One Month Ended 10/31/2024

					10	**FY 2024**
Description	YTD FS Per General Ledger	Eliminate Rev Deduct & Other Inc	Adj Rev Deduct to RHC Calc	Cost Report Allocations	RHC Financial Statements	"Annualized" RHC Financial Statements
Gross Patient Revenue	178,808	-	-	-	178,808	214,569
Less: Revenue deductions	143,170	(143,170)	169,870	-	169,870	203,844
Net Patient Revenue	321,978	(143,170)	169,870	-	348,678	418,413
Other Income (if any)	2,512	(2,512)	-	-	-	-
Operating revenue	324,490	(145,682)	169,870	-	348,678	418,413
Operating Expenses:						
Salaries	218,697	-	-	-	218,697	262,436
Benefits	30,822	-	-	-	30,822	36,987
Prof Fees	750	-	-	34,601	35,351	42,421
Contract Labor	14,978	-	-	-	14,978	17,974
Purch Serv	62,474	-	-	-	62,474	74,969
Supplies	10,823	-	-	-	10,823	12,987
Rent	20,116	-	-	-	20,116	24,139
Utilities	7,529	-	-	-	7,529	9,035
Repairs	1,076	-	-	-	1,076	1,292
Other	5,220	-	-	-	5,220	6,264
Insurance	2,254	-	-	-	2,254	2,705
Travels & Meals	987	-	-	-	987	1,184
Management Fee Direct Exp	-	-	-	115,403	115,403	138,484
Critical Access Hospital Overhead Allocation (a)	-	-	-	184,113	184,113	220,936
Total Operating Expenses	375,727	-	-	334,117	709,844	851,813
Net Income (loss)	**(51,237)**	**(145,682)**	**169,870**	**(334,117)**	**(361,166)**	**(433,400)**

MGMT Fee Allocation est. 2023	1 months	11,540
IP Rounding allocation based on 8/31/22 IRR estimate	8 months	27,681
CAH Overhead Allocation - from Chris based on last filed cost report -------->	12 months	220,936
Total allocation ------->		260,157

Item 8.

Mangum RHC Reimbursement Analysis 4

(a) Will experience increased volumes from swing-bed rounding in FY2023 One Month Ended 10/31/2024

9.75 9.95

	VOLUMES: Current Month				VOLUMES: Year-To-Date 09-30-24			
Payer	Clinic (On-Site)	Telehealth	Swing-Bed (a)	TOTAL	Clinic (On-Site)	Telehealth	Swing-Bed (a)	TOTAL
MCR	**58**		**4**	62	**360**		**54**	414
MCR Managed Care	**4**			4	**46**		**17**	63
Medicaid	**14**			14	**330**			330
BCBS	**31**			31	**250**			250
Commercial	**80**			80	**399**			399
Self-Pay	**8**			8	**63**		**3**	66
Other				-	**-**			-
	195	-	4	199	1,448	-	74	1,522

	Projected Reimbursement Rate			***Projected Reimbursement***			
MCR	**$ 367.66**	**$ -**	**$ 367.66**	132,358	-	19,854	152,211
MCR Managed Care	**$ 367.66**	**$ -**	**$ 367.66**	16,912	-	6,250	23,163
Medicaid	**$ 367.66**	**$ -**	**$ 367.66**	121,328	-	-	121,328
BCBS	**$ 73.00**		**$ -**	18,250			18,250
Commercial	**$ 73.00**		**$ -**	29,127	-	-	29,127
Self-Pay	**$ 73.00**		**$ -**	4,599	-	-	4,599
Other	**$ 73.00**		**$ -**	-	-	-	-
				$ 322,574	$ -	$ 26,104	$ 348,678

Clinic (On-Site)	# of Accounts at + or - $5 balance	Total Cash Received	Average Payment per Visit
MCR			<-- use RHC rate
MCR Managed Care			<-- use RHC rate
Medicaid			<-- use RHC rate
BCBS			#DIV/0!
Commercial			#DIV/0!
Self-Pay			#DIV/0!
Other			#DIV/0!

Telehealth	# of Accounts at + or - $5 balance	Total Cash Received	Average Payment per Visit
MCR			
MCR Managed Care			
Medicaid			
BCBS			#DIV/0!
Commercial			#DIV/0!
Self-Pay			#DIV/0!
Other			#DIV/0!

Latest filed cost report:		FY24 Proj	
Cost	**$ 709,844**	**$ 851,813**	
Visits	**1,522**	**1,826**	<-- excl Telehealth.
MCR rate	***$ 466.39***	***$ 466.39***	
2024 CAP RATE	***$ 338.62***	***$ 367.66***	
12/19/23	New Rate per (2024)	**$ 282.65**	

Item 8.

VENDOR NAME	DESCRIPTION	0-30 Days	31-60 Days	61-90 Days	OVER 90 Days	10/31/2024	9/30/2024	8/31/2024	7/31/2024
ALCO SALES & SERVICE CO	Patient Supplies	-	-	-	-	-	-	-	-
ADVANCED MEDICAL SALES, INC	Patient Supplies	-	-	-	-	-	215.44	-	-
ALPHACARD	Supplies	-	-	-	-	-	-	245.98	-
AMERICAN HEART ASSOCIATION INC	Supplies	-	-	-	-	-	-	-	-
AMERICAN PROFICIENCY INSTITUTE	Lab Supplies	-	-	-	-	-	-	-	-
AMERISOURCE RECEIVABLES (ARFC)	Pharmacy Supplies	186.04	-	-	-	186.04	-	-	-
ANESTHESIA SERVICE INC	Patient Supplies	-	-	-	-	-	-	926.00	200.00
APEX MEDICAL GAS SYSTEMS, INC	Supplies	-	-	-	-	-	-	-	-
ARAMARK	Linen Services	-	-	-	-	-	-	-	-
ASD HEALTHCARE	Pharmacy Supplies	327.69	-	-	-	327.69	-	-	-
ASPEN INSPECTION SERVICES	Repairs/maintenance	-	-	-	-	-	-	-	-
AT&T	Fax Service	2,147.88	-	-	-	2,147.88	295.53	1,892.76	-
AVANAN, INC.	COVID Capital	-	-	-	-	-	16,800.00	16,800.00	16,800.00
BARRY DAVENPORT	1099 Provider	-	-	-	-	-	-	-	-
BIO-RAD LABORATORIES INC	Lab Supplies	-	-	-	-	-	-	2,297.26	963.30
BRIGGS HEALTHCARE	Supplies	-	-	-	-	-	-	-	-
CARNEGIE EMS	Patient Transport Svs	-	-	-	-	-	-	-	-
CARNEGIE TRI-COUNTY MUN. HOSP	Pharmacy Supplies	1,192.26	-	-	-	1,192.26	-	-	-
CARRIER CORP	Shipping	-	-	-	-	-	-	-	-
CDW-G LLC	Supplies	-	-	-	-	-	-	-	-
CENTRAL STATES RECOVERY	Collections	102.50	-	-	-	102.50	99.88	-	-
CITY OF MANGUM	Utilities	-	-	-	-	-	-	-	7,657.27
CLIA LABORATORY PROGRAM	Lab Services	-	-	-	-	-	-	-	-
CliftonLarsonAllen LLP	Audit firm	-	-	-	-	-	-	-	-
COHESIVE HEALTHCARE MGMT	Mgmt Fees	230,073.11	231,146.80	230,288.64	2,263,640.70	2,955,149.25	2,950,076.14	2,849,370.08	2,823,640.79
COHESIVE HEALTHCARE RESOURCES	Payroll	-	-	-	4,352,383.45	4,352,383.45	4,354,367.04	4,766,078.72	4,964,216.59
COHESIVE MEDIRYDE LLC	Patient Transportation Service	1,370.25	-	-	-	1,370.25	-	786.25	-
COHESIVE STAFFING SOLUTIONS	Agency Staffing Service	1,097,886.84	778,078.28	766,374.07	4,003,202.28	6,645,541.47	6,195,671.04	5,843,680.38	5,543,592.33
COMMERCIAL MEDICAL ELECTRONICS	Quarterly Maintenance	1,750.00	-	-	-	1,750.00	-	-	-
CORRY KENDALL, ATTORNEY AT LAW	Legal Fees	-	-	-	-	-	-	-	-
CPSI	EHR Software	-	-	-	-	-	-	-	-
CURBELL MEDICAL PRODUCTS INC	Supplies	-	-	-	-	-	-	-	-
DAN'S HEATING & AIR CONDITIONI	Repairs/maintenance	4,880.00	-	-	-	4,880.00	-	-	-
DELL FINANCIAL SERVICES LLC	Server Lease	-	-	-	-	-	-	-	-
DIAGNOSTIC IMAGING ASSOCIATES	Radiology Purch Svs	2,150.00	-	-	-	2,150.00	2,150.00	2,150.00	2,150.00
DOERNER SAUNDERS DANIEL ANDERS	Legal Fees	-	-	-	358,558.16	358,558.16	358,558.16	358,558.16	358,558.16
DR W. GREGORY MORGAN III	1099 Provider	-	-	-	-	-	-	-	-
DYNAMIC ACCESS	Vascular Consultant	750.00	-	-	-	750.00	1,400.00	-	1,500.00
eCLINICAL WORKS, LLC	RHC EHR	-	-	-	-	-	-	1,960.79	-
EMD MILLIPORE CORPORATION	Lab Supplies	-	-	-	-	-	-	-	-
ENTRUSTED TRANSPORT, LLC	Patient Transportation Service	-	-	-	-	-	349.34	-	-
EOI INC	Patient Equipment	3,431.12	-	-	-	3,431.12	-	-	-
EQUALIZERCM REVOPS	Business Office Services	58,782.61	-	-	-	58,782.61	-	-	-
F1 INFORMATION TECHNOLOGIES IN	IT Support Services	-	-	-	-	-	-	-	-
FEDEX	Shipping	84.77	-	-	-	84.77	-	90.18	43.07
FFF ENTERPRISES INC	Pharmacy Supplies	-	648.20	-	-	648.20	3,178.20	1,881.80	-
FIRE EXTINGUISHER SALES & SERV	Maintenance Supplies	182.50	-	-	-	182.50	-	-	-
FIRSTCARE MEDICAL SERVICES, PC	1099 Provider	-	-	-	-	-	-	-	-
FIRST DIGITAL COMMUNICATIONS	IT Support Services	1,634.92	-	-	-	1,634.92	-	-	-
FORVIS LLP	Finance Purch Svs(Formerly BKD)	-	-	-	-	-	-	-	-
FOX BUILDING SUPPLY	Repairs/maintenance	-	-	-	-	-	-	-	-
FUCHS RADIO, LLC	Advertising	110.00	-	-	-	110.00	-	110.00	-
GEORGE BROS TERMITE & PEST CON	Pest Control Service	365.00	-	-	-	365.00	-	165.00	165.00
GLOBAL EQUIPMENT COMPANY INC.	Patient Supplies	-	-	-	-	-	-	-	-
GRAINGER	Maintenance Supplies	-	-	-	-	-	-	-	1,039.11
GREER COUNTY CHAMBER OF	Advertising	-	-	-	-	-	-	-	-

Item 8.

VENDOR NAME	DESCRIPTION	0-30 Days	31-60 Days	61-90 Days	OVER 90 Days	10/31/2024	9/30/2024	8/31/2024	7/31/2024
GREER COUNTY TREASURER	Insurance	-	-	-	-	-	-	-	-
HAC INC	Dietary Supplies	179.77	-	-	-	179.77	-	35.61	223.64
HEALTH CARE LOGISTICS	Pharmacy Supplies	-	-	-	-	-	-	-	-
HEARTLAND PATHOLOGY CONSULTANT	Lab Consultant	-	-	-	-	-	-	-	1,050.00
HENRY SCHEIN	Lab Supplies	-	-	-	-	-	-	-	-
HEWLETT-PACKARD FINANCIAL SERV	Computer Services	307.10	-	-	-	307.10	307.10	307.10	307.10
HILL-ROM COMPANY, INC	Rental Equipment	-	-	-	-	-	-	-	-
HOBART SERVICE	Repairs/maintenance	-	-	-	-	-	-	-	-
HOSPITAL EQUIPMENT RENTAL COMP	Rental Equipment	3,155.00	-	-	-	3,155.00	3,155.00	3,155.00	-
ICU MEDICAL SALES INC.	Supplies	-	-	-	-	-	-	-	-
HSI	Materials Purch svs	3,000.00	-	-	-	3,000.00	-	-	-
IMPERIAL, LLC.-LAWTON	Dietary Purchased Service	-	-	-	-	-	-	-	-
INQUISEEK LLC	RHC purch svs	-	-	-	-	-	225.00	225.00	225.00
INSIGHT DIRECT USA INC.	IT Minor Equipment	-	-	-	-	-	-	-	-
JANUS SUPPLY CO	Housekeeping Supplies, based in Altus	-	-	-	-	-	751.14	636.20	973.25
JIMALL & KANISHA' LOFTIS	Rent House	-	-	-	-	-	(850.00)	(850.00)	(850.00)
KCI USA	Rental Equipment	889.95	-	-	-	889.95	-	-	-
KELLEY MARTINEZ	Expense Reimbursement	344.59	-	-	-	344.59	-	-	-
KING GUIDE PUBLICATIONS INC	Advertising	-	-	-	-	-	-	-	-
LABCORP	Lab purch svs	-	-	-	-	-	-	-	-
LAMPTON WELDING SUPPLY	Patient Supplies	-	-	-	-	-	-	155.00	-
LANGUAGE LINE SERVICES INC	Translation service	-	-	-	-	-	-	-	130.00
LG PRINT CO	Advertising	-	-	-	-	-	-	-	-
LOCKE SUPPLY	Plant Ops supplies	857.86	-	-	-	857.86	-	-	309.65
MANGUM STAR NEWS	Advertising	-	-	-	-	-	-	-	41.16
MARK CHAPMAN	Employee Reimbursement	-	-	-	-	-	-	-	-
MCKESSON / PSS - DALLAS	Patient Care/Lab Supplies	-	-	-	-	-	7,719.80	3,381.44	1,473.58
MCKESSON - 340 B	Pharmacy Supplies	1,093.24	-	-	-	1,093.24	3,704.41	319.35	0.06
MEDLINE INDUSTRIES	Patient Care/Lab Supplies	20,121.24	-	-	-	20,121.24	10,744.68	14,415.31	8,315.95
MYHEALTH ACCESS NETWORK, INC	Compliance purch svs	758.95	-	-	-	758.95	758.95	758.95	758.95
NATHAN ANDREW PERRY	Biomed Services	-	-	-	-	-	-	-	-
NATIONAL RECALL ALERT CENTER	Safety and Compliance	-	-	-	-	-	-	-	-
NEXTIVA, INC.	Phone Svs	-	-	-	-	-	-	-	-
NUANCE COMMUNICATIONS INC	RHC purch svs	79.00	-	-	-	79.00	-	-	123.00
OFMQ	Quality purch svs	-	-	-	-	-	-	-	-
OHERI	Education/Training	-	-	-	-	-	-	-	-
OKLAHOMA BLOOD INSTITUTE	Blood Bank	-	-	-	-	-	-	-	-
OPTUM	Pharmacy Supplies	-	-	-	-	-	-	-	-
ORGANOGENESIS INC	Patient Care/Lab Supplies	-	-	-	-	-	-	-	-
ORTHO-CLINICAL DIAGNOSTICS INC	Lab purch svs	-	-	-	-	-	-	-	-
PARA REV LOCKBOX	CDM purch svs	-	-	-	-	-	-	-	2,909.00
PHARMA FORCE GROUP LLC	340B purch svs	-	-	-	-	-	1,161.79	-	1,148.32
PHARMACY CONSULTANTS, INC.	PHARMACY CONSULTANTS, INC.	3,445.86	-	-	-	3,445.86	2,600.00	2,600.00	3,467.79
PHILADELPHIA INSURANCE COMPANY	OHA Insurance	7,720.50	-	-	-	7,720.50	-	-	-
PHILIPS HEALTHCARE	Supplies	-	-	-	-	-	-	-	-
PIPETTE COM	Lab maintenance	-	-	-	-	-	-	116.00	116.00
PITNEY BOWES GLOBAL FINANCIAL	Postage rental	-	-	-	-	-	-	-	-
PORT53 TECHNOLOGIES, INC.	Software license	-	-	-	-	-	-	-	-
PRESS GANEY ASSOCIATES, INC	Purchased Service	-	-	-	-	-	-	-	738.40
PUCKETT DISCOUNT PHARMACY	Pharmacy Supplies	-	-	-	-	-	-	-	-
PURCHASE POWER	Postage Fees	-	-	-	-	-	-	-	-
RADIATION CONSULTANTS	Radiology maintenance	-	-	-	-	-	-	3,250.00	-
RESPIRATORY MAINTENANCE INC	Repairs/maintenance	-	-	-	-	-	-	-	-
REYES ELECTRIC LLC	COVID Capital	-	-	-	-	-	-	4,000.00	11,100.00
RUSHMORE TRANSPORT LLC	Patient Transportation Service	-	-	-	-	-	-	-	-
RUSSELL ELECTRIC & SECURITY	Repair and Maintenance	-	-	-	-	-	770.00	-	-

Item 8.

VENDOR NAME	DESCRIPTION	0-30 Days	31-60 Days	61-90 Days	OVER 90 Days	10/31/2024	9/30/2024	8/31/2024	7/31/2024
SBM MOBILE PRACTICE, INC	1099 Provider	-	-	-	-	-	-	-	-
SCHAPEN LLC	Clinic Rent	-	-	-	-	-	(1,750.00)	(1,750.00)	(1,750.00)
SECURITY CHECK	Security	70.00	-	-	-	70.00	-	-	-
SHERWIN-WILLIAMS	Supplies	-	-	-	-	-	(11.78)	(11.78)	(11.78)
SHRED-IT USA LLC	Secure Doc disposal service	-	-	-	-	-	-	-	-
SIEMENS HEALTHCARE DIAGNOSTICS	Service Contract	22,034.78	(12,735.48)	-	-	9,299.30	(12,735.48)	18,620.66	9,859.11
SIZEWISE	Rental Equipment	-	-	-	-	-	-	-	-
SMAART MEDICAL SYSTEMS INC	Radiology interface/Radiologist provider	1,735.00	-	-	-	1,735.00	-	1,735.00	1,735.00
SOMSS LLC	1099 Provider	-	-	-	-	-	-	-	-
SPACELABS HEALTHCARE LLC	Telemetry Supplies	-	-	-	-	-	-	-	-
SPARKLIGHT BUSINESS	Cable service	-	-	-	-	-	-	-	-
STANDLEY SYSTEMS LLC	Printer lease	-	-	-	-	-	587.10	-	2,241.50
STAPLES ADVANTAGE	Office Supplies	543.35	-	-	-	543.35	208.74	1,194.13	903.17
STERICYCLE INC	Waste Disposal Service	-	-	-	-	-	-	-	1,476.24
STERICYCLE / SHRED-IT	Waste Disposal Service	1,245.16	-	-	-	1,245.16	-	-	-
STRYKER INSTRUMENTS	Patient Supplies	-	-	-	-	-	-	-	-
SUMMIT UTILITIES	Utilities	-	-	-	-	-	-	-	750.17
TECUMSEH OXYGEN & MEDICAL SUPP	Patient Supplies	-	-	-	-	-	-	-	-
THERMO FISHER SCIENTIFIC LLC	Lab Supplies	392.55	-	-	-	392.55	-	-	-
TIGER ATHLETIC BOOSTERS	Advertising	-	-	-	-	-	-	-	-
TOUCHPOINT MEDICAL, INC	Med Dispense Monitor Support	-	-	-	-	-	3,285.00	3,285.00	3,285.00
TRIOSE INC	Freight	116.70	-	-	-	116.70	-	40.14	1,176.54
TRS MANAGED SERVICES	Agency Staffing-old	-	-	-	-	-	-	-	-
TRUBRIDGE	Software license	-	-	-	-	-	-	234.00	451.41
ULINE	Patient Supplies	513.82	-	-	-	513.82	-	1,713.20	603.50
ULTRA-CHEM INC	Housekeeping Supplies	-	-	-	-	-	-	-	-
US FOODSERVICE-OKLAHOMA CITY	Food and supplies	-	-	(7.84)	-	(7.84)	(7.84)	(7.84)	525.51
US MED-EQUIP LLC	Swing bed eq rental	-	-	-	-	-	-	-	-
VITAL SYSTEMS OF OKLAHOMA, INC	Swing bed purch service	-	-	-	-	-	-	-	-
WELCH ALLYN, INC.	Supplies	-	-	-	-	-	-	-	-
WORTH HYDROCHEM	semi-annual water treatment	-	-	-	-	-	-	-	-
BLUTH FAMILY MEDICINE, LLC	1099 Provider	-	-	-	-	-	-	-	-
CARDINAL HEALTH 110, LLC	Patient Supplies	3,752.42	-	-	-	3,752.42	-	5,098.09	670.05
CUSTOM MEDICAL SOLUTIONS	Equipment Rental Agreement	-	(948.00)	-	-	(948.00)	(948.00)	-	(1,125.00)
DATA CENTER WAREHOUSE LLC	Equipment Rental Agreement	-	-	-	-	-	-	-	-
DIRECTV	Cable service	294.55	-	-	-	294.55	-	288.30	-
SOUTHWEST TAB & COMMISSIONING	Repairs/maintenance	-	-	-	-	-	-	-	-
VESTIS	Housekeeping Service	9,771.39	-	-	-	9,771.39	9,771.39	13,028.52	9,742.05
ZOLL MEDICAL CORP.	Patient Supplies	-	-	-	-	-	-	-	-
BADGE BUDDIES LLC	Office Supplies	-	-	-	-	-	-	-	-
CARLOS MENDOZA	Education/Training	-	-	-	-	-	-	-	-
CULLIGAN WATER CONDITIONING	Equipment Rental Agreement	-	-	-	-	-	-	-	-
DELL MARKETING L.P	Server Lease	-	-	-	-	-	830.00	-	-
DP MEDICAL SERVICES	Rental	-	-	-	-	-	-	-	-
FEDEX FREIGHT	Shipping	147.76	-	-	-	147.76	-	147.76	-
FREEBORN DYSPHAGIA ASSOC LLC	1099 Provider	-	-	-	-	-	-	-	-
PYA, P.C.	Audit firm	-	-	-	-	-	-	-	-
							-	-	-
Grand Total		**1,489,978.03**	**996,189.80**	**996,654.87**	**10,977,784.59**	**14,460,607.29**	**13,913,437.77**	**13,923,113.50**	**13,783,618.94**
			Reconciling Items:		Conversion Variance	13,340.32	13,340.32	13,340.32	13,340.32
					AP Control	14,447,266.97	14,792,821.21	14,802,496.94	14,663,002.38
					Accrued AP	1,560,236.01	836,719.58	828,360.35	712,075.16
					AHSO Related AP	(892,723.76)	(892,723.76)	(892,723.76)	(892,723.76)
					TOTAL AP	**15,114,779.22**	**14,736,817.03**	**14,738,133.53**	**14,482,353.78**
						15,114,779.22	14,736,817.03	14,738,133.53	14,482,353.78
						-	-	-	-

IT Security Supply Chain OT Security Insider Threat Physical Security Interoperable Communications

Item 9.

DEFEND TODAY, SECURE TOMORROW

CYBER INFRASTRUCTURE SURVEY

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE CYBER INFRASTRUCTURE SURVEY (CIS) ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTED BY REGIONALLY-LOCATION CYBERSECURITY ADVISORS, A CIS EVALUATES THE EFFECTIVENESS, RESILIENCE AND CYBERSECURITY PREPAREDNESS OF AN ORGANIZATION'S SECURITY CONTROLS.

FORMAT AND GOAL

A CIS is a facilitated, expert-led assessment with cybersecurity personnel from your organization (e.g., Chief Information Security Officer, ICS/SCADA Security Manager, IT Security Manager). This informal interview typically takes 2½ to 4 hours in length.

Its goal is to assess the foundational and essential cybersecurity practices of an organization's critical service to identify dependencies, capabilities and emerging effects of the current cybersecurity posture. After the survey, DHS will provide an interactive dashboard for scenario planning.

APPROACH

CIS focuses on a service-based-view versus a programmatic-view of cybersecurity. Critical services are assessed against more than 80 cybersecurity controls grouped under five top-level domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.

Following the assessment, DHS will provide a user friendly dashboard for reviewing and interacting with the survey findings. Your organization can use the dashboard to compare its results against its industry peers, review results in the context of specific cyber and physical threat scenarios, and dynamically adjust the importance of in-place practices to see the effects on overall cyber protection.

CYBERSECURITY FRAMEWORK

The cybersecurity controls surveyed within the CIS broadly align to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), but does not show an organization's adherence to the NIST CSF. The CIS computes a unique, service-specific cyber protective resilience index based on only a narrow set of cyber protection and resilience measures. The NIST CSF is a comprehensive framework and should be considered as a next step after leveraging the CIS results.

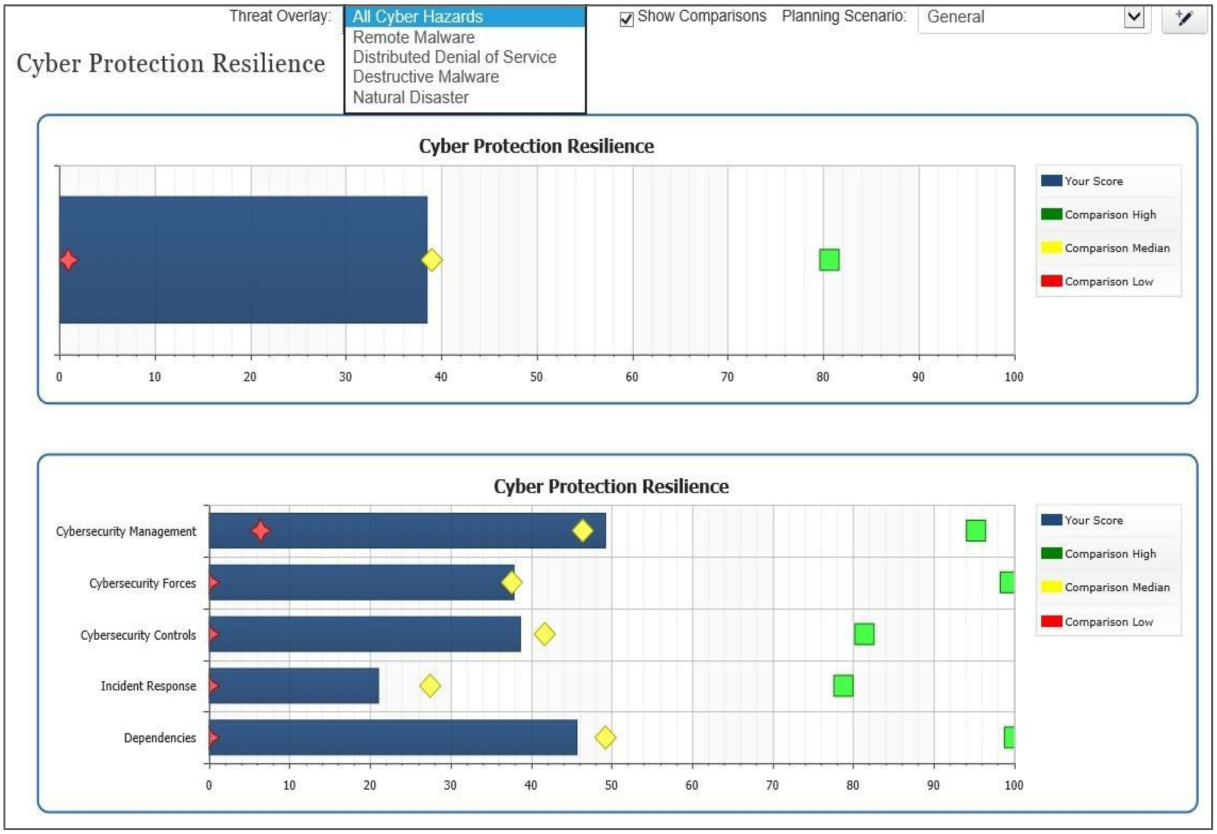
BENEFITS AND OUTCOMES

A CIS provides your organization with:

- An effective assessment of cybersecurity controls in-place for critical service;
- A user friendly, interactive dashboard to support cybersecurity planning and resource allocation; and
- Access to peer performance data, visually depicted on the dashboard.

DATA PRIVACY

The CIS dashboard is for your organization’s exclusive use. All data collected and analysis performed during the CIS is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.



CIS Survey Question Domains

CIS Domains

Cybersecurity Forces

- Personnel
- Cybersecurity Training

Cybersecurity Controls

- Authentication and Authorization Controls
- Access Controls
- Cybersecurity Measures
- Information Protection
- User Training
- Defense Sophistication and Compensating Controls

Incident Response

- Incident Response Measures
- Alternate Site and Disaster Recovery

Cybersecurity Management

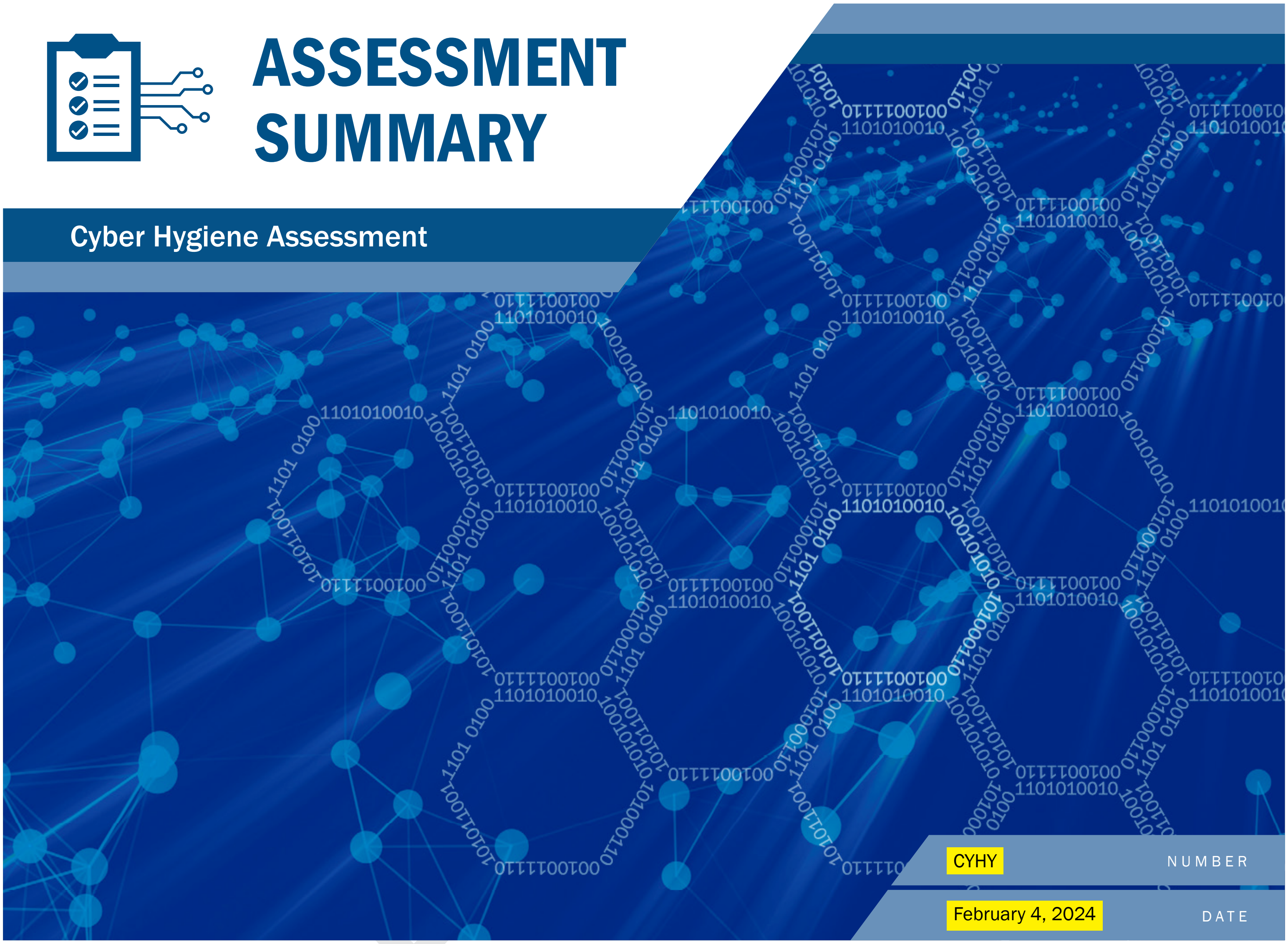
- Cybersecurity Leadership
- Cyber Service Architecture
- Change Management
- Lifecycle Tracking
- Assessment and Evaluation
- Cybersecurity Plan
- Cybersecurity Exercises
- Information Sharing

Dependencies

- Data at Rest
- Data in Motion
- Data in Process
- End Point Systems

For further information, contact your Cybersecurity Advisor (CSA) at iodregionaloperations@cisa.dhs.gov.

ASSESSMENT SUMMARY



Cyber Hygiene Assessment

CYHY NUMBER

February 4, 2024 DATE

Cyber Hygiene Assessment

Sample Organization

CISA
CYBER+INFRASTRUCTURE

Contents

List of Figures

List of Tables

Item 9.

1 How To Use This Report

Welcome to your Cyber Hygiene (CyHy) report. This document aims to be a comprehensive weekly snapshot of known vulnerabilities detected on Internet-facing hosts for Sample Organization (SAMPLE).

You may wonder what you're supposed to do with all this information. While it's not our intent to prescribe to you a particular process for remediating vulnerabilities, we hope you'll use this report to strengthen your security posture. Here's a basic flow:

1. Review the Cyber Hygiene Report Card for a high-level overview. This section gives a quick comparison of the problems we find week to week. If this is your first report, you should note that the Report Card will initially lack historical data to make comparisons against, though that data will exist in your next report.
2. Review the Emergency Directive 19-01 — New Certificates Summary for current certificate information. This section gives a quick look at the currently expired, soon to expire, and newly added certificates for known hostnames owned by or managed on behalf of your organization.
3. See Appendix A: Vulnerability Summary for a list of unique vulnerabilities across all the systems we detect problems with. Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability provides more information about each vulnerability and all the hosts that we detect are susceptible to a given vulnerability. You should focus on those vulnerabilities rated with the greatest severity, as well as those that impact your high-value assets, but don't ignore the medium or low vulnerabilities. Recognize that a vulnerability's rating tends to get worse with time.
4. If this report is not your first, review Appendix B: Vulnerability Changes Since Last Report for a breakdown of all the changes we detected in your scope in the last week.
5. If you've patched a vulnerability since your last report, verify it's listed here. If it's not present, there may still be an issue. It may also be possible that the issue was fixed after our latest scan, which was on February 4, 2024.
6. For additional analysis, see Appendix G: Attachments, which provides Comma-Separated Values (CSV) files for all findings, services, hosts, and the scope that we scan.
7. Review Appendix E: False Positive Findings to track any upcoming expiration dates for false positive designations. For any new false positives, please complete and return the False Positive Assertion Form found in Appendix G: Attachments to the Cybersecurity and Infrastructure Security Agency (CISA).

You should be aware that Cyber Hygiene does not scan your entire scope (all of the addresses your organization has sent us) every week, but does attempt to scan every host each week. For an explanation of how CyHy works, see the Methodology section.

As you review the report, you may have additional questions. Check out the answers we provide in the Frequently Asked Questions section. If you have any additional questions, email us at vulnerability@cisa.dhs.gov.

1.1 SAMPLE Points of Contact

SAMPLE has defined the following points-of-contact for Cyber Hygiene activities; if present, reports are emailed solely to distribution lists. If you receive this report through a distribution list, the CISA requests that you funnel your request through your technical POC(s).

Type	Name	Email Address	Phone Number
Technical	Technical POC 1	tech_poc_1@sample.org	555-555-1111
Technical	Technical POC 2	tech_poc_2@sample.org	555-555-2222
Technical	Technical POC 3	tech_poc_3@sample.org	555-555-3333
Technical	Technical POC 4	tech_poc_4@sample.org	555-555-4444
Distribution List	Distro POC 1	distro_poc_1@sample.org	

CYBER HYGIENE

REPORT CARD

Sample Organization

0 Hosts with unsupported software

37 Potentially Risky Open Services

3% Decrease in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

November 6, 2023 — February 4, 2024
Completed host scan on all assets

January 26, 2024 — February 4, 2024
Last vulnerability scan on all hosts

ASSETS OWNED

220,807
No Change

ASSETS SCANNED

220,807
No Change
100% of assets scanned

HOSTS

827 ↓
Decrease of **10**

SERVICES

2,413 ↑
Increase of **33**

VULNERABLE HOSTS

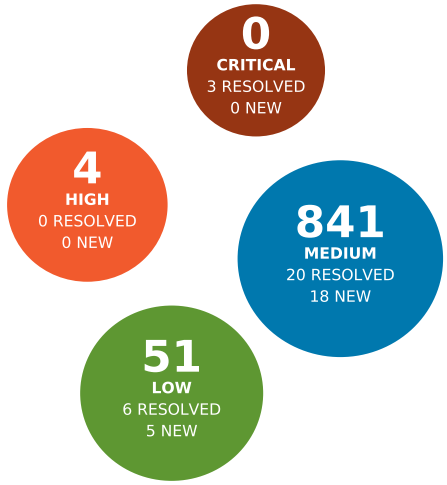
268 ↓
Decrease of **6**
32% of hosts vulnerable

VULNERABILITIES

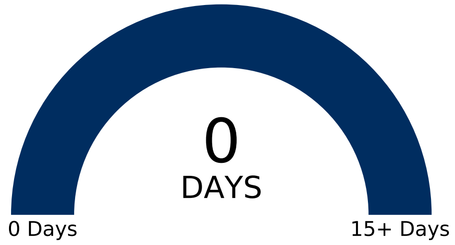
896 ↓
Decrease of **6**

VULNERABILITIES

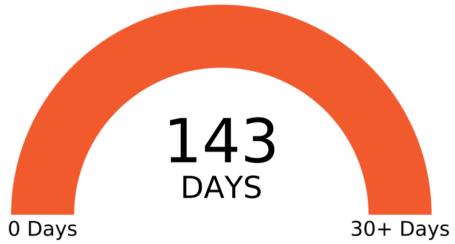
SEVERITY BY PROMINENCE



VULNERABILITY RESPONSE TIME



MAX AGE OF ACTIVE CRITICALS



MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

●	RDP* 0	■	FTP 4
■	Telnet* 11	▲	RPC 1
●	SMB* 0	▲	SQL 4
●	LDAP 0	●	IRC 0
▲	NETBIOS 3	▲	Kerberos 14

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

** Denotes the possibility of a network management interface.*

3 Binding Operational Directive 22-01 — Reducing the Significant Risk of Known Exploited Vulnerabilities

Malicious cyber campaigns frequently use Known Exploited Vulnerabilities (KEVs) to threaten the public sector, the private sector, and ultimately the security and privacy of individual citizens. Therefore it is essential to quickly remediate KEVs to protect federal information systems and reduce cyber incidents.

CISA issued Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilties to evolve the federal government's approach to vulnerability management and keep pace with threat activity. The directive establishes a CISA managed catalog of known exploited vulnerabilities and requires federal civilian agencies to identify and remediate these vulnerabilities found on your information systems within two weeks.

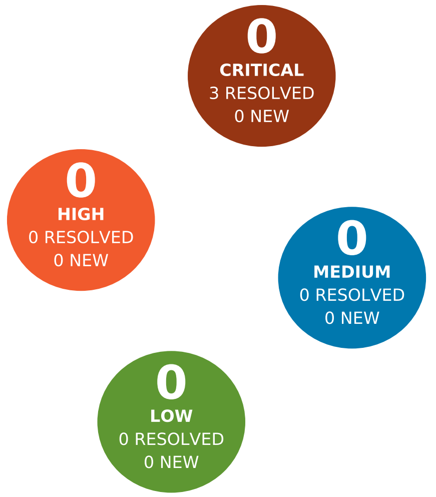
CISA updates this catalog with new vulnerabilities when the following conditions are met:

- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID.
- There is reliable evidence that the vulnerability has been actively exploited in the wild.
- There is a clear remediation action for the vulnerability, such as a vendor provided update.

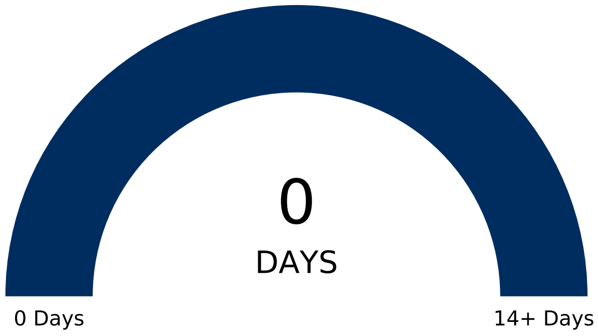
To report newly exploited vulnerabilities that are not in this catalog, please email CISA Central at central@cisa.dhs.gov.

Details on the below findings can be found in "findings.csv" in Appendix G.

KEV SEVERITY BY PROMINENCE



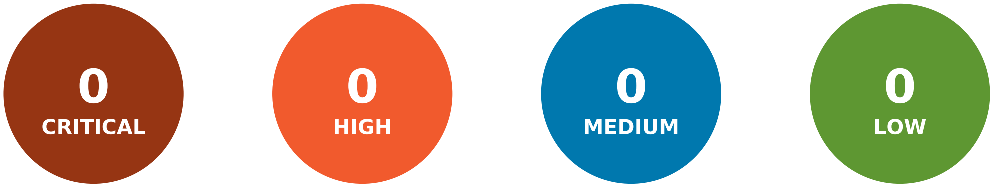
KEV RESPONSE TIME



MAX AGE OF ACTIVE KEVS

Signed into law in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) required CISA to establish the Ransomware Vulnerability Warning Pilot (RVWP). The goal of the RVWP is to warn organizations about exposed vulnerabilities that may be exploited by ransomware threat actors.

Of the **0** KEV findings detected on SAMPLE's internet-facing assets, **0** are known by CISA to have been used in ransomware campaigns.



4 Binding Operational Directive 23-02 — Mitigating the Risk from Internet-Exposed Management Interfaces

Threat actors often use certain classes of network devices to gain unrestricted access to organizational networks leading to full scale compromises. Inadequate security, misconfigurations, and out-of-date software make these devices more vulnerable to exploitation. The risk is further compounded if device management interfaces are connected directly to, and accessible from, the public-facing Internet. Most device management interfaces are designed to be accessed from dedicated physical interfaces and/or management networks and are not meant to be accessible directly from the public Internet.

CISA issued Binding Operational Directive (BOD) 23-02 to push the federal government to take steps toward reducing the attack surface created by insecure or misconfigured management interfaces across certain classes of devices. The BOD requires networked management interfaces (NMIs) using certain protocols over the Internet to be removed from the public Internet or to be protected by capabilities that enforce access control to the interface through a policy enforcement point separate from the interface itself as part of a Zero Trust Architecture (ZTA) within 14 days of discovery.

We also recommend reviewing all hosts with potentially risky open services, especially if they are functioning as networked management interfaces, to ensure that each service is intended to be available to the public and, where applicable, the service is up to date on the latest version, correctly configured, and uses strong authentication.

You can find a list of potentially risky services detected as available on your external network within this report's "potentially-risky-services.csv" attachment. In it, there is a column which denotes those that may be associated with NMIs to help with prioritization.

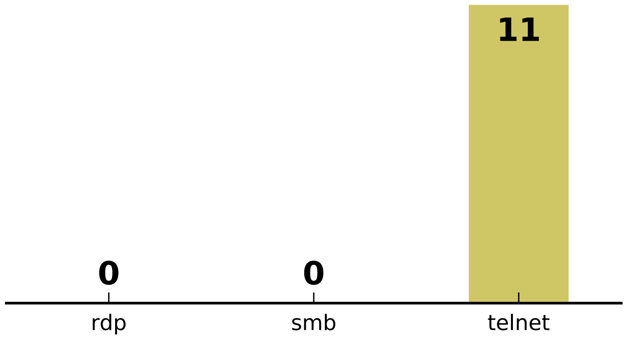


Figure 1: Potential Network Management Interface (NMI) Service Counts

The details for these findings can be found within the "potentially-risky-services.csv" file located in Appendix G: Attachments. You will need to ensure you open the report with a dedicated PDF reader (such as Adobe Acrobat), and click on the paper clip icon to the left of the CSV file in order to open it.

Item 9.

5 Emergency Directive 19-01 — New Certificates Summary

Issued on 22 January 2019, Emergency Directive (ED) 19-01 requires CISA to assist Federal agencies in identifying newly added certificates to Certificate transparency (CT) logs for agency domains. CISA is supporting the directive by providing certificate information found in CT log entries for known agency second-level domains and all subdomains under them. Per the directive, agencies shall monitor CT log data for certificates issued that they did not request. Detailed information on the certificates discovered by CISA can be found in the `certificates.csv` attachment within the agency's weekly Cyber Hygiene report.

We recommend focusing on validating that newly-added certificates were purposefully issued; new certificates issued without a known purpose may indicate Domain Name Service (DNS) infrastructure tampering. The issuing organization table is included to help identify possible outlier certificates that have been issued by an unusual organization.

HIGH LEVEL FINDINGS

UNEXPIRED CERTIFICATES	LATEST SCAN DATE
47	February 4, 2024

NEW CERTIFICATES ISSUED

CURRENT FISCAL YEAR	LAST 30 DAYS	LAST 7 DAYS
50	20	7

CERTIFICATE EXPIRATION

EXPIRED IN LAST 7 DAYS	EXPIRED IN LAST 30 DAYS	EXPIRING IN 7 DAYS	EXPIRING IN 30 DAYS
2	12	4	11

Issuing Agency	Number of Certificates
CN=R3,O=Let's Encrypt,C=US	17
CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	7
CN=E1,O=Let's Encrypt,C=US	7
CN=GTS CA 1P5,O=Google Trust Services LLC,C=US	6
CN=Sectigo ECC Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	6
CN=Amazon RSA 2048 M02,O=Amazon,C=US	1
CN=Entrust Certification Authority - L1K,OU=(c) 2012 Entrust\, Inc. - for authorized use only,OU=See www.entrust.net/legal-terms,O=Entrust\, Inc.,C=US	1
CN=GeoTrust RSA CA 2018,OU=www.digicert.com,O=DigiCert Inc,C=US	1
CN=DigiCert EV RSA CA G2,O=DigiCert Inc,C=US	1

Item 9.

6 Executive Summary

This report provides the results of a CISA CyHy assessment of SAMPLE conducted from November 6, 2023 at 15:42 UTC through February 4, 2024 at 17:33 UTC. The Cyber Hygiene assessment includes network mapping and vulnerability scanning for Internet-accessible SAMPLE hosts. This report is intended to provide SAMPLE with enhanced understanding of their cyber posture and to promote a secure and resilient Information Technology (IT) infrastructure across SAMPLE's Internet-accessible networks and hosts.

For this reporting period, a total of 827 hosts were identified out of the 220,807 addresses provided to CISA. The scanning revealed 896 total potential vulnerabilities on 268 vulnerable hosts, 32% of all SAMPLE hosts. 258 distinct open ports, 183 distinct services, and 64 operating systems were detected.

30 distinct types of potential vulnerabilities (0 critical, 2 high, 20 medium, and 8 low) were detected, as shown in Table 2. The vulnerabilities that were detected most frequently on SAMPLE hosts are displayed in Figure 2.

SAMPLE should review the potential vulnerabilities detected and report any false positives back to CISA so they can be excluded from future reports. Please refer to Appendix A: Vulnerability Summary for an illustration of the breakdown of vulnerability occurrences over time.

Severity	Distinct Vulnerabilities		Total Vulnerabilities	
Critical	0%	0	0%	0
High	7%	2	0%	4
Medium	67%	20	94%	841
Low	27%	8	6%	51
Total		30		896

Table 2: Number of Vulnerabilities by Severity Level

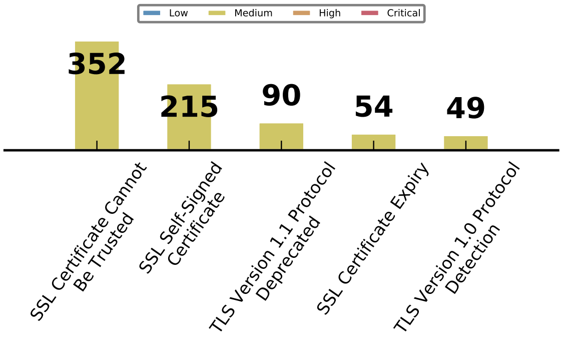


Figure 2: Top Vulnerabilities by Occurrence

Additionally, the top high-risk hosts and top risk-based vulnerabilities are displayed in Figure 3 and Figure 4. For more information about these risk calculations, refer to Table 9: Risk Rating System.

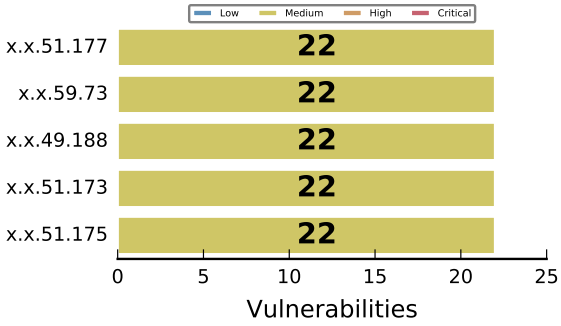


Figure 3: Top High-Risk Hosts

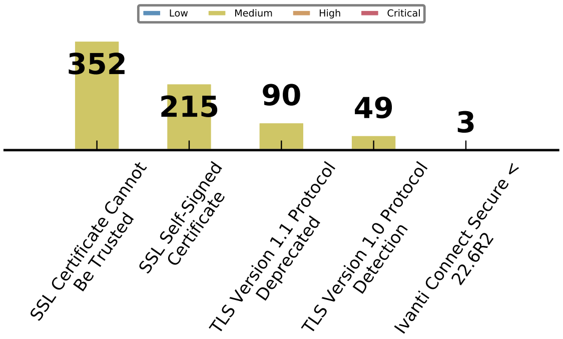


Figure 4: Top Risk-Based Vulnerabilities

⚠ 7 false positive finding(s) expire within 30 days.
See Appendix E.1: Expiring Soon False Positive Findings for more information.

The most frequently detected operating systems and services for SAMPLE are displayed in Table 3 and Table 4 respectively.

Operating System	Detections	
unknown	63.1%	1,188
FreeBSD 6.2-RELEASE	18.5%	348
Oracle Solaris 11	4.4%	83
OpenBSD 4.0	3.6%	67
Linux 2.6.32	0.9%	17
Other	9.6%	181

Table 3: Top Operating Systems Detected

Service	Detections	
https	21.9%	486
http-proxy	16.1%	358
jetdirect	11.5%	256
http	11.3%	251
websocket	3.6%	80
Other	35.5%	787

Table 4: Top Services Detected

The next two figures illustrate how quickly SAMPLE responds to vulnerabilities that have been identified. Figure 5 shows how long it has taken SAMPLE to mitigate vulnerabilities of each severity level (for vulnerabilities mitigated since February 4, 2023), while Figure 6 shows the median ages of current active vulnerabilities. Vulnerability age is based on the initial detection date by CyHy.

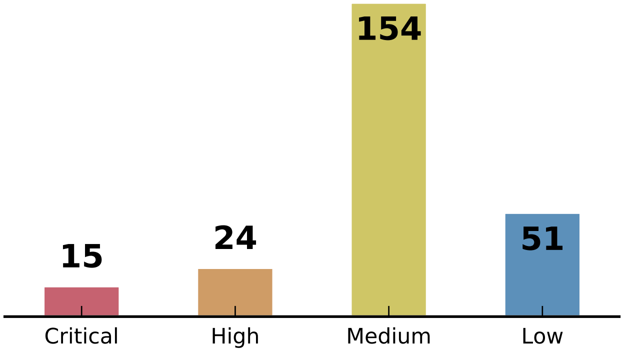


Figure 5: Median Time in Days to Mitigate Vulnerabilities

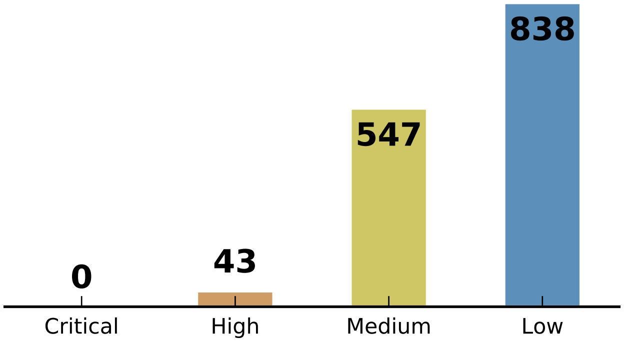


Figure 6: Median Age in Days of Active Vulnerabilities

Figure 7 displays the number of active critical vulnerabilities that were less than 30 days old and more than 30 days old, as of the date indicated on the graph. Vulnerability age is based on the initial detection date by CyHy.

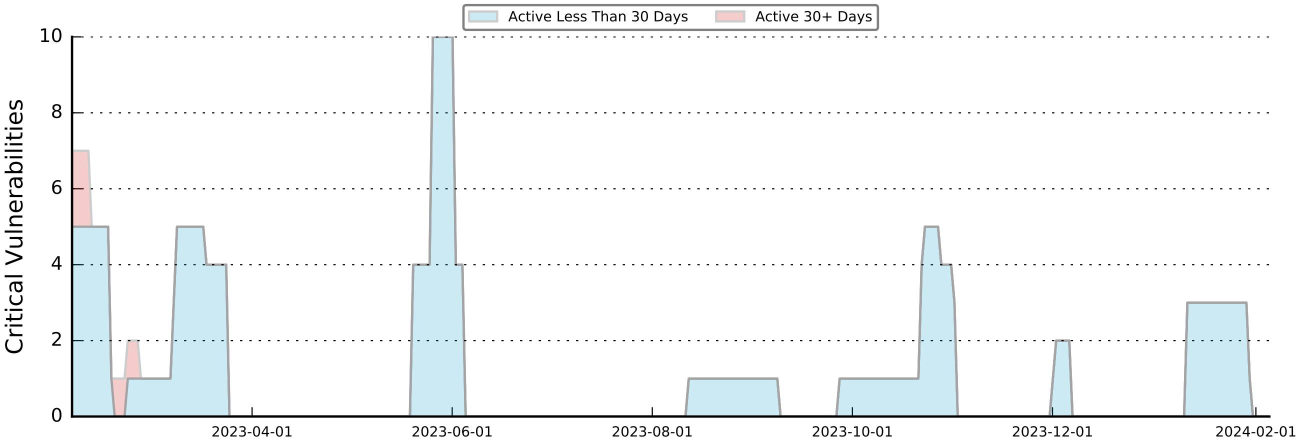


Figure 7: Critical Vulnerability Age Over Time

Figure 8 and Table 5 provide an age breakdown of every currently active critical vulnerability for SAMPLE.

No Critical Vulnerabilities Detected
Figure Omitted

Figure 8: Active Critical Vulnerability Age

	0-7 Days	7-14 Days	14-21 Days	21-30 Days	30-90 Days	90+ Days
Active Critical Vulnerabilities	0	0	0	0	0	0

Table 5: Active Critical Vulnerability Age Summary

7 Sub-Organization Summary

This section shows the key CyHy metrics for each sub-organization within SAMPLE. A CSV with this data can be found in Appendix G: Attachments.

Org	Addresses		Hosts		Vulnerabilities Detected				Services	Median Days To Mitigate				Median Days Currently Active			
Name	Owned	Scanned	Detected	Vulnerable	Critical	High	Med	Low	Detected	Critical	High	Med	Low	Critical	High	Med	Low
SUB_ORG	65,630	100%	77	27 (35%)	0	0	49	5	144	16	35	204	273	0	0	546	126
SUB_ORG	628	100%	42	8 (19%)	0	0	12	0	62	0	0	186	31	0	0	138	0
SUB_ORG	2,175	100%	25	1 (4%)	0	0	2	0	37	444	0	232	13	0	0	851	0
SUB_ORG	77,779	100%	93	53 (57%)	0	0	113	5	241	6	7	118	114	0	0	213	139
SUB_ORG	0	0%	0	0 (0%)	0	0	0	0	0	0	0	0	0	0	0	0	0
SUB_ORG	66	100%	7	5 (71%)	0	0	6	9	12	0	0	46	0	0	0	548	1,349
SUB_ORG	73,233	100%	458	131 (29%)	0	1	522	27	1,571	0	39	135	49	0	143	547	813
SUB_ORG	178	100%	18	5 (28%)	0	0	6	2	57	30	55	236	337	0	0	630	506
SUB_ORG	68	100%	13	8 (62%)	0	0	88	0	118	15	15	84	0	0	0	355	0
SUB_ORG	40	100%	16	6 (38%)	0	0	8	0	30	0	0	471	0	0	0	786	0
SUB_ORG	96	100%	73	21 (29%)	0	0	35	3	134	0	5	260	76	0	0	664	852
SUB_ORG	17	100%	1	0 (0%)	0	0	0	0	2	0	0	0	0	0	0	0	0
SUB_ORG	897	100%	4	3 (75%)	0	3	0	0	5	18	0	37	0	0	43	0	0
SAMPLE Total	220,807	100%	827	268 (32%)	0	4	841	51	2,413	15	24	154	51	0	43	547	838

8 Methodology

8.1 Background

CISA conducted a Cyber Hygiene assessment of SAMPLE's Internet-facing networks and hosts from November 6, 2023 at 15:42 UTC through February 4, 2024 at 17:33 UTC. This report provides result summaries and detailed findings of the CyHy assessment activity for SAMPLE and its associated sub-organizations. All scan results are included in Appendix G: Attachments as CSV files.

Cyber Hygiene is intended to improve your security posture by proactively identifying and reporting on vulnerabilities and configuration issues present on Internet-facing systems before those vulnerabilities can be exploited.

Cyber Hygiene is a service provided by the Cybersecurity and Infrastructure Security Agency (CISA).

CISA began Cyber Hygiene in January 2012 to assess, on a recurring basis, the "health" of unclassified federal civilian networks accessible via the Internet. Since then, the program has grown to provide a persistent scanning service to federal, state, local, tribal, and territorial governments and private sector organizations.

Upon submission of an Acceptance Letter, SAMPLE provided CISA with their public network address information. SAMPLE and CISA agreed on any time restrictions which would be imposed on the scanning activity.

8.2 Process

All Cyber Hygiene scanning activity originates from a dynamic set of Amazon Web Services (AWS) Internet Protocol (IP) addresses in the US East and US West regions. The live list of active addresses can be found at https://rules.ncats.cyber.dhs.gov. The addresses in that list will change based on overall CyHy scan demand.

CyHy uses a combination of scanning services for testing:

- Network Mapping
- Vulnerability Scanning

Network Mapping

Using Nmap [https://nmap.org], we attempt to determine what hosts are available, identify what services (application name and version) those hosts are offering, and what Operating System (OS) versions they are running. We first scan the most commonly detected 1,000 Transmission Control Protocol (TCP) ports of the addresses you've submitted to us to get a quick understanding of the active/dark landscape. An address that has a least one port open/listening service is considered a *host* and is then fully port-scanned (TCP) and included in the vulnerability scan. For the purposes of this report, *tcpwrapped* ports are not considered to be open; for more information on tcpwrapped ports, refer to the Frequently Asked Questions section.

If no services are detected in the most common 1,000 ports on a given IP address, that address is considered "dark" in CyHy and will be re-scanned after at least 90 days to check for change. Addresses marked dark are not included in the host count of the weekly report. Understand that CyHy is not attempting to make a judgment call about why an address is unresponsive. If there's not a port open, it's not a *host* in the language of CyHy.

Vulnerability Scanning

Using Nessus, a commercial vulnerability scanner, each host is evaluated against a library of vulnerabilities that an Internet-based actor could exploit. Vulnerabilities are reported with a severity of critical, high, medium, or low to facilitate prioritization of remediation efforts. We enable all Nessus Plugins [https://www.tenable.com/plugins/] except those in the “Denial of Service” family.

Scanning Frequency

Scanning occurs continuously between each weekly report. All hosts are scanned for vulnerabilities at least once every two weeks; hosts with vulnerabilities are scanned more frequently.

Cyber Hygiene’s scan prioritization is as follows:

- Addresses with no running services detected (dark space) are rescanned after at least 90 days.
- Hosts with no vulnerabilities detected are rescanned every 7 days.
- Hosts with low-severity vulnerabilities are rescanned every 6 days.
- Hosts with medium-severity vulnerabilities are rescanned every 4 days.
- Hosts with high-severity vulnerabilities are rescanned every 24 hours.
- Hosts with critical-severity vulnerabilities are rescanned every 12 hours.

You should understand that a single host may have multiple vulnerabilities of varying severity, which impacts the frequency that the host is scanned.

To be clear, it is not the case that we scan your entire address scope for vulnerabilities each week (unless each address you’ve provided to us has a responsive host). It is the case, though, that each host will get vulnerability scanned at least once per week.

Recurring Vulnerabilities

After you’ve remediated a vulnerability (and it remains resolved for a period of 90 days), the host’s scan priority will drop. This approach allows CISA to focus on the areas of importance and give more attention to the hosts that need it.

Vulnerabilities are assigned an age in order to track timeliness of remediation. Vulnerability age is determined by when it was first detected on a host, not from when it first appeared on a report. As scanning occurs continuously between weekly reports, it is possible to have “new” vulnerabilities appear on a report that are already days old. It is also possible for a vulnerability to fluctuate between being detected and not detected during mid-week scans and then at a future time appear in a report as many days old. If a mitigated vulnerability is re-detected less than 90 days after the date of non-detection, it will be considered to be the same vulnerability with the same “initial detection date” as previously recorded. If it is re-detected more than 90 days after the date of non-detection, it will be treated as a new vulnerability with a new “initial detection date”.

Vulnerability Scoring

The Nessus vulnerability scanner references the National Vulnerability Database (NVD) [https://nvd.nist.gov/] for its vulnerability information. The NVD provides CVSS scores for many known vulnerabilities. In particular, NVD supports the CVSS version standard for all CVE vulnerabilities.

The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. The NVD uses severity rankings of “Low”, “Medium”, “High”, and “Critical” in addition to the numeric CVSS scores, but these qualitative rankings are simply mapped from the numeric CVSS base scores.

Within this report, qualitative severity rankings are determined primarily by a vulnerability’s CVSSv3 base score. If a CVSSv3 base score has not been assigned to a vulnerability, but a CVSSv2 base score has, this report will use the CVSSv2 base score to determine the severity rating with the exception that a base score of 10 will be reported as “Critical.” Where the NVD has not provided a CVE severity rating, this report relies on the Nessus scanner’s own rating.

What’s In The Report?

Though Cyber Hygiene initiates multiple scans between reports, *only the latest scan data for each host is used to determine current vulnerability*. This is the data that appears in the main body of the report and in Appendix A: Vulnerability Summary, Appendix B.2: New Vulnerabilities Detected and Appendix B.3: Re-Detected (Previously-Mitigated) Vulnerabilities.

If a vulnerability was detected since that last report (e.g., it wasn’t in the previous report’s findings, though CyHy saw it mid-week) but it was not in the latest scan, we include it in Appendix B.4: Recently-Detected Vulnerabilities.

If a vulnerability that was previously reported to you is no longer detected by the latest scan, the vulnerability and host will be listed in Appendix B.1: Mitigated Vulnerabilities.

We encourage you to validate the status of vulnerabilities in both Appendix B.1: Mitigated Vulnerabilities and Appendix B.4: Recently-Detected Vulnerabilities against your change control register. This will help to ensure that the vulnerability we detected has actually been remediated and is not simply unresponsive to our scans.

9 Approximate Host Locations

The map below shows the approximate locations of detected hosts as listed in a geo-location database. This map is provided as a tool to identify hosts that may have been mistakenly added in to, or removed from scope. The map is scaled to include all known SAMPLE host locations.

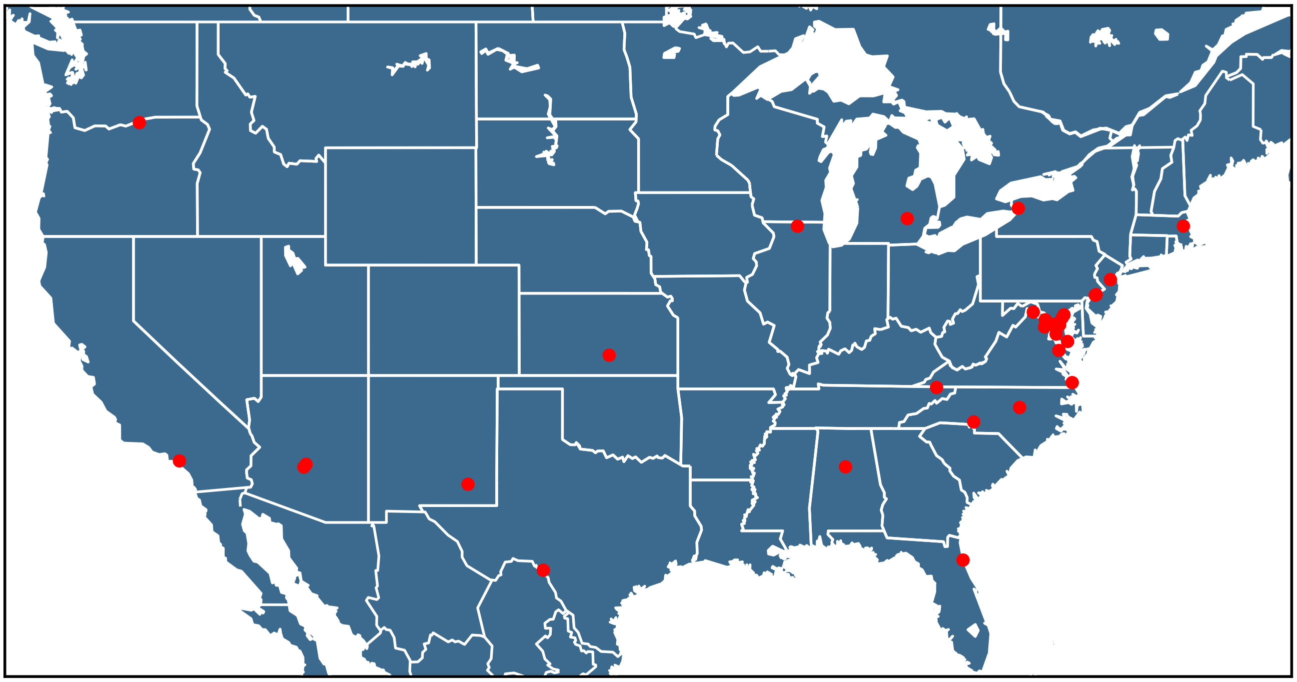


Figure 9: Approximate Host Locations

Item 9.

10 Vulnerability Scan Results

For this period, CyHy detected 896 occurrences of 30 distinct vulnerabilities (0 critical, 4 high, 841 medium, and 51 low). SAMPLE should review the vulnerabilities detected and report any false positives back to CISA so these can be excluded from future reports (see the Frequently Asked Questions section for more about false positives).

The scanning detected 268 vulnerable hosts—242 hosts with one to five vulnerabilities were identified; 2 hosts had between six and nine vulnerabilities; 24 hosts had ten or more vulnerabilities identified.

Severity	Distinct Vulnerabilities		Total Vulnerabilities	
Critical	0%	0	0%	0
High	7%	2	0%	4
Medium	67%	20	94%	841
Low	27%	8	6%	51
Total		30		896

Table 6: Number of Vulnerabilities by Severity Level

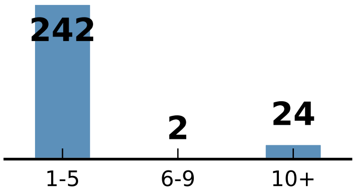


Figure 10: Vulnerability Count per Host

The CVSS scores for all active vulnerabilities can be found in Figure 11.

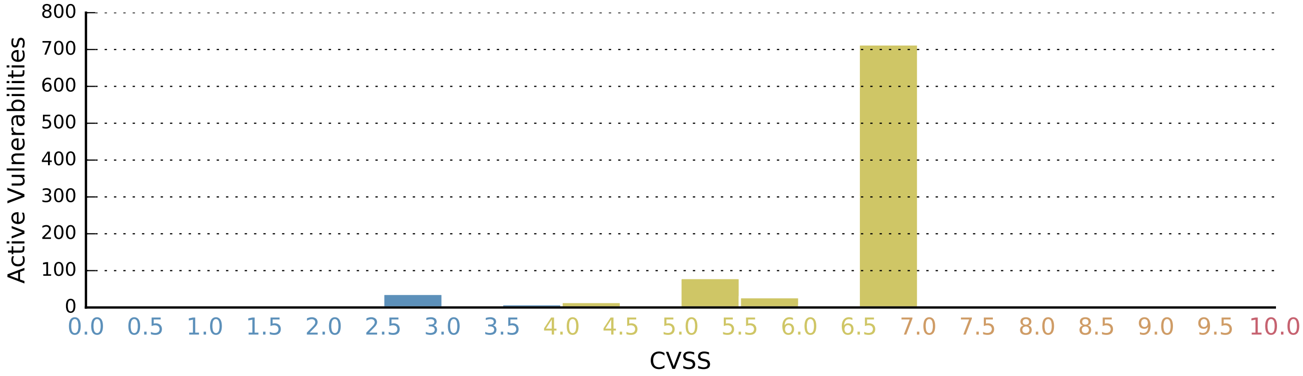


Figure 11: CVSS Histogram for Active Vulnerabilities

The top vulnerabilities according to CVSS score are represented in Table 7.

Vulnerability Name	Severity	Hosts	CVSS Score
Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	3	7.8
Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	1	7.5
SSL Certificate Cannot Be Trusted	Medium	352	6.5
SSL Self-Signed Certificate	Medium	215	6.5
TLS Version 1.1 Protocol Deprecated	Medium	90	6.5
TLS Version 1.0 Protocol Detection	Medium	49	6.5
HSTS Missing From HTTPS Server (RFC 6797)	Medium	8	6.5
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	4	6.1
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	17	5.9
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	11	5.9

Table 7: Top Vulnerabilities by CVSS

A complete list of distinct vulnerabilities detected, including severity level and number of hosts having the vulnerability can be found in Appendix A: Vulnerability Summary. Full details on every detected vulnerability can be found in Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability. Every critical and high finding detected, along with the hosts that have these findings, are listed in Appendix D: Critical and High Vulnerability Mitigations by IP Address.

The top high-risk hosts are identified in Table 8 by combining the total number of vulnerabilities, the severity of the vulnerabilities, and a weighted CVSS score for vulnerabilities detected. For more information on the formula, please refer to Table 9: Risk Rating System.

IP Address	Critical	High	Medium	Low	Total
x.x.51.177	0	0	22	0	22
x.x.59.73	0	0	22	0	22
x.x.49.188	0	0	22	0	22
x.x.51.173	0	0	22	0	22
x.x.51.175	0	0	22	0	22
x.x.51.176	0	0	22	0	22
x.x.51.32	0	0	22	0	22
x.x.59.76	0	0	22	0	22
x.x.59.75	0	0	22	0	22
x.x.59.74	0	0	22	0	22

Table 8: Top Hosts by Weighted Risk

The Risk Rating System (RRS) emphasizes higher-rated CVSS scores to ensure that hosts with a large number of lower-risk vulnerabilities do not outweigh hosts with a smaller number of high-risk vulnerabilities, while ensuring that hosts with an extreme number of low-risk vulnerabilities are not overshadowed by hosts with a single higher-risk issue. The RRS also ensures that hosts with a significant number of high-risk vulnerabilities will not be overshadowed by a host with only a single critical vulnerability.

Table 9 illustrates the base and weighted CVSS scores and shows the equivalent number of lower-risk vulnerabilities to weigh evenly with a single critical (CVSS score of 10) vulnerability.

Base CVSS Score	Weighted CVSS Score	Equivalent to CVSS Score 10
1.0	1×10^{-06}	10,000,000.0
2.0	0.000,128	78,125.0
3.0	0.002,187	4,572.47
4.0	0.016,384	610.35
5.0	0.078,125	128.0
6.0	0.279,936	35.72
7.0	0.823,543	12.14
8.0	2.097,152	4.77
9.0	4.782,969	2.09
10.0	10.0	1.0

Table 9: Risk Rating System

As an example, a host having 400 vulnerabilities with a base CVSS score of 1.0 would get a weighted RRS score of 4×10^{-04}, which is considered lower-risk than a host with a single critical vulnerability (RRS score of 10.0). Similarly, a host having 4 vulnerabilities with a base CVSS score of 8 would get a RRS score of 8.39 and still be considered a lower risk than a host with a single critical vulnerability (RRS score of 10.0).

11 Results Trending

To help decision-makers, this section provides a comparison of the current data against similar CyHy scans conducted over time.

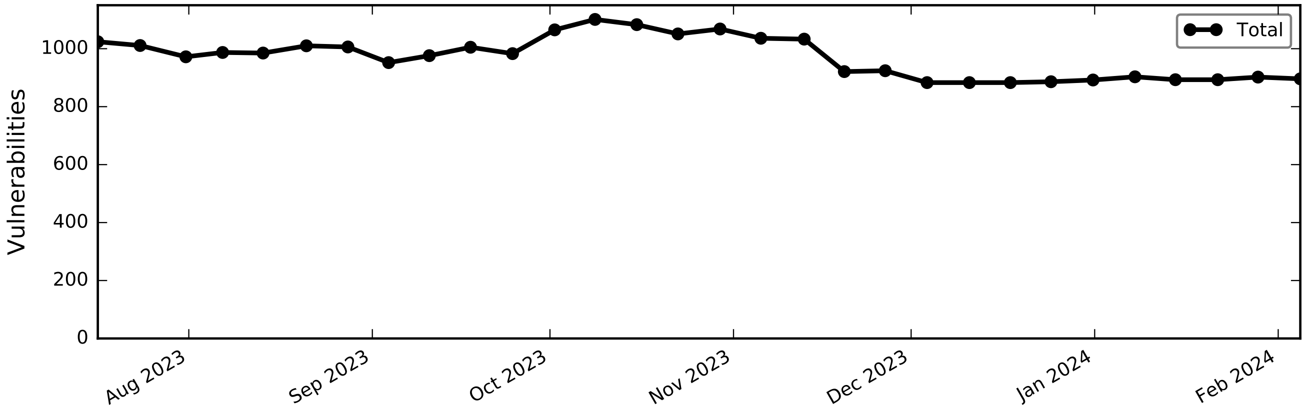


Figure 12: Total Active Vulnerabilities Over Time

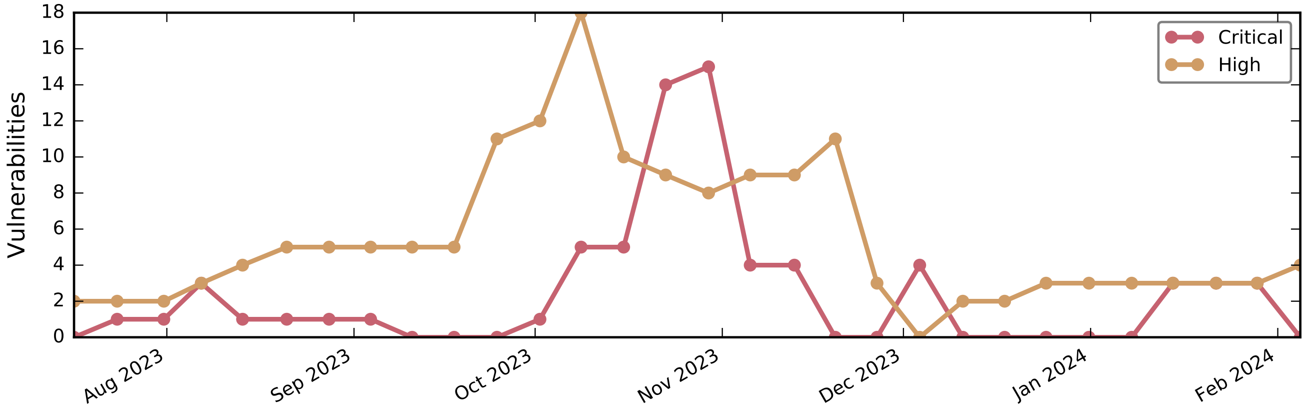


Figure 13: Active Critical and High Vulnerabilities Over Time

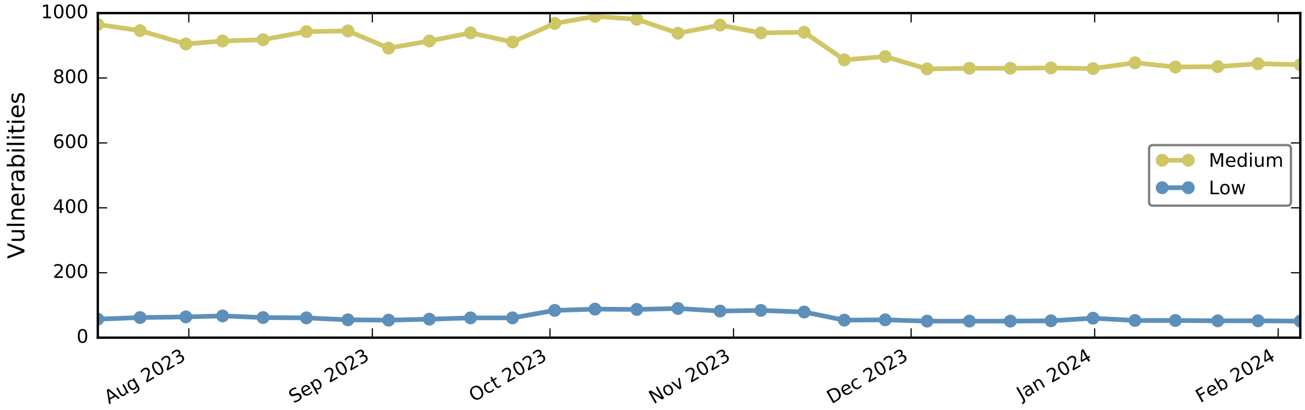


Figure 14: Active Medium and Low Vulnerabilities Over Time

SAMPLE vulnerability profile over time, reporting on the total hosts detected, number of hosts with vulnerabilities, number of distinct services, and the number of distinct vulnerabilities detected can be found in Figure 15, Figure 16, and Figure 17 respectively.

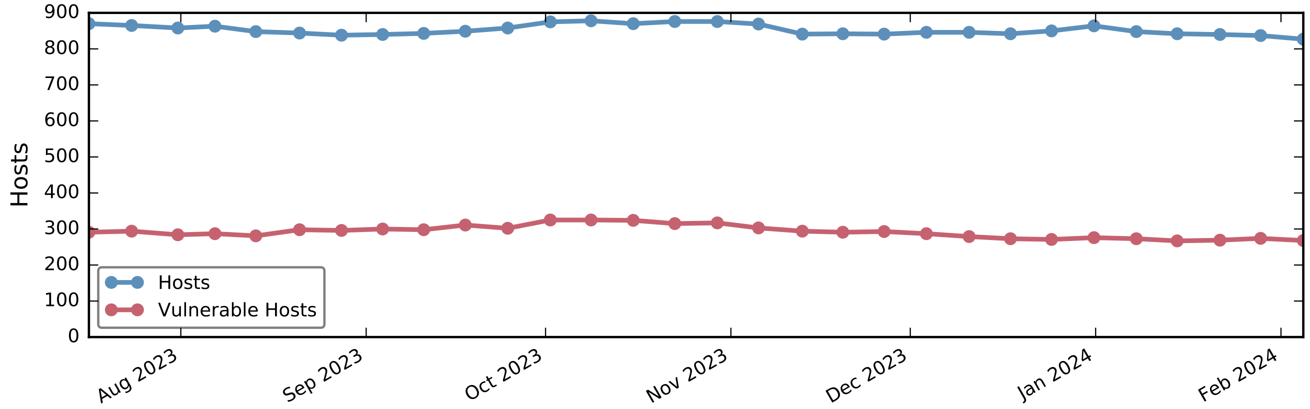


Figure 15: Vulnerable Hosts Over Time

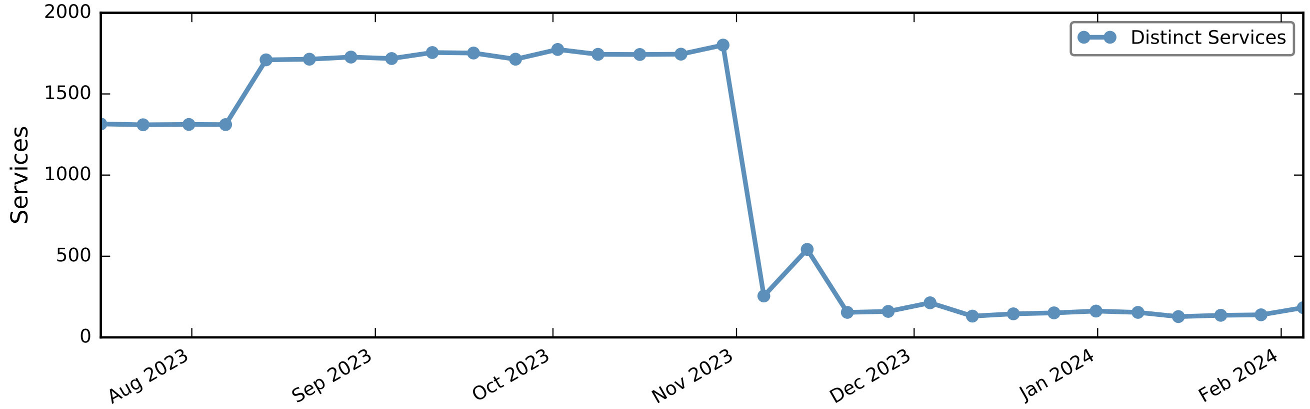


Figure 16: Distinct Services Over Time

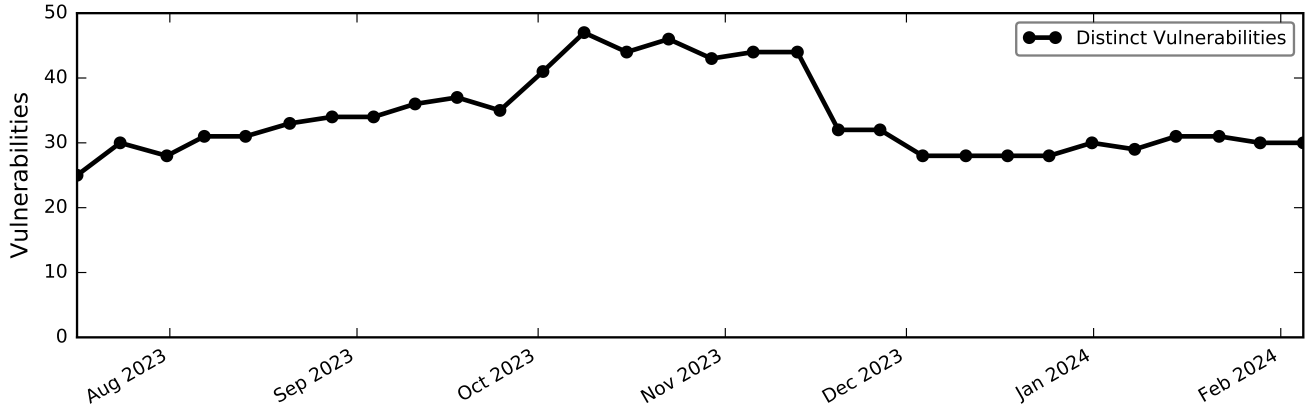


Figure 17: Distinct Vulnerabilities Over Time

Item 9.

	Previous Report	Current Report	% Change
Hosts	837	827	-2.0%
Vulnerable Hosts	274	268	-3.0%
Distinct Services	139	183	31.0%
Distinct Vulnerabilities	30	30	0.0%
Distinct Operating Systems	67	64	-5.0%

Table 10: Comparison with Previous Report

Overall, for all hosts identified, SAMPLE averaged 1.08 vulnerabilities per host. For vulnerable hosts, SAMPLE averaged 3.34 total vulnerabilities per host. By severity, vulnerable hosts averaged 0.0 critical, 0.01 high, 3.14 medium, and 0.19 low vulnerabilities per host.

12 Conclusion

SAMPLE should use the data provided in this report to correct any identified vulnerabilities, configuration errors, and security concerns in your external network perimeter. If SAMPLE has questions, comments, or concerns about the findings or data contained in this report, please work with your designated technical point of contact when requesting assistance from CISA at vulnerability@cisa.dhs.gov.

Appendix A Vulnerability Summary

This section presents counts of all distinct vulnerabilities that were detected in the latest scans. It shows the name of the vulnerability, the severity level of the vulnerability, and the number of vulnerability detections in the previous report vs. this report. Low, medium, high, and critical vulnerabilities are displayed.

Vulnerability	Severity	Previous	Current	Change
Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	3	0	-100.0%
Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	1	1	0.0%
Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	3	3	0.0%
Web Application Potentially Vulnerable to Clickjacking	Medium	1	3	200.0%
Backup Files Disclosure	Medium	6	7	16.7%
HSTS Missing From HTTPS Server (RFC 6797)	Medium	7	8	14.3%
TLS Version 1.0 Protocol Detection	Medium	48	49	2.1%
HTTP TRACE / TRACK Methods Allowed	Medium	10	10	0.0%
SSH Weak Algorithms Supported	Medium	2	2	0.0%
F5 BIG-IP Cookie Remote Information Disclosure	Medium	2	2	0.0%
Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	Medium	2	2	0.0%
Nonexistent Page (404) Physical Path Disclosure	Medium	1	1	0.0%
Sun ONE Application Server Upper Case Request JSP Source Disclosure	Medium	1	1	0.0%
Apache Tomcat Default Files	Medium	2	2	0.0%
IIS Detailed Error Information Disclosure	Medium	3	3	0.0%
OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	8	8	0.0%
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	11	11	0.0%
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	17	17	0.0%
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	4	4	0.0%
TLS Version 1.1 Protocol Deprecated	Medium	90	90	0.0%
SSL Self-Signed Certificate	Medium	216	215	-0.5%
SSL Certificate Cannot Be Trusted	Medium	355	352	-0.8%
SSL Certificate Expiry	Medium	57	54	-5.3%
SSL Anonymous Cipher Suites Supported	Low	2	3	50.0%
Web Server Allows Password Auto-Completion	Low	4	5	25.0%
SSH Server CBC Mode Ciphers Enabled	Low	6	6	0.0%
SSH Weak MAC Algorithms Enabled	Low	7	7	0.0%
SSH Weak Key Exchange Algorithms Enabled	Low	7	7	0.0%
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	2	2	0.0%
Web Server HTTP Header Internal IP Disclosure	Low	19	18	-5.3%
Web Server Load Balancer Detection	Low	5	3	-40.0%

Appendix B Vulnerability Changes Since Last Report

B.1 Mitigated Vulnerabilities

This section lists the vulnerabilities that were included on the previous report, but were not detected by the latest scans. The table provides the initial detection and mitigation detection dates, plus the number of days it took to mitigate each vulnerability.

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.151	443	2024-01-11	2024-01-30 00:01	18
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.152	443	2024-01-11	2024-01-30 04:43	18
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.20.200	443	2024-01-11	2024-01-30 00:02	18
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.121	8443	2024-01-27	2024-01-31 23:36	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.75	443	2023-09-16	2024-01-29 17:08	136
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	443	2021-10-06	2024-02-02 20:58	849
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	8883	2022-08-05	2024-02-02 20:58	547
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.59	443	2024-01-21	2024-01-29 13:25	8
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.52.116	4502	2024-01-26	2024-01-30 18:42	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.52.117	4502	2024-01-26	2024-01-30 07:36	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.77	1805	2022-08-05	2024-02-01 01:07	545
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.151	4502	2024-01-26	2024-01-30 15:23	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.152	4502	2024-01-26	2024-01-30 15:41	4
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.183	443	2023-12-19	2024-02-03 02:54	46
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.145	443	2016-07-21	2024-01-29 11:39	2748
SUB_ORG	SSL Certificate Expiry	Medium	x.x.52.116	4502	2024-01-26	2024-01-30 18:42	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.52.117	4502	2024-01-26	2024-01-30 07:36	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.60.151	4502	2024-01-26	2024-01-30 15:23	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.60.152	4502	2024-01-26	2024-01-30 15:41	4
SUB_ORG	SSL Certificate Expiry	Medium	x.x.60.34	443	2024-01-26	2024-01-30 13:35	4
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.108.121	8443	2024-01-27	2024-01-31 23:36	4
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.59.77	1805	2022-08-05	2024-02-01 01:07	545
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.108.121	8443	2024-01-27	2024-01-31 23:36	4
SUB_ORG	Web Server Allows Password Auto-Completion	Low	x.x.108.75	443	2023-09-16	2024-01-29 17:08	136
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.149	443	2021-10-06	2024-02-02 20:58	849
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.52.213	443	2024-01-24	2024-02-01 13:17	8
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.60.227	443	2024-01-24	2024-02-01 15:04	8
SUB_ORG	Web Server Load Balancer Detection	Low	x.x.50.53	443	2023-05-27	2024-01-29 22:43	247

Owner	Vulnerability	Severity	Host	Port	Initial Detection	Mitigation Detected (UTC)	Days To Mitigate
SUB_ORG	Web Server Load Balancer Detection	Low	x.x.89.152	443	2022-12-16	2024-01-29 19:33	409

B.2 New Vulnerabilities Detected

This section lists the new vulnerabilities that were detected for the first time in the latest scans. The table provides the initial detection and latest detection dates for each vulnerability.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)
SUB_ORG	HSTS Missing From HTTPS Server (RFC 6797)	Medium	x.x.80.167	443	2024-02-04 07:11	2024-02-04 07:11
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.253	443	2024-02-03 12:30	2024-02-03 12:30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.69	443	2024-02-04 03:53	2024-02-04 03:53
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.55	443	2024-01-31 07:40	2024-02-04 17:05

B.3 Re-Detected (Previously-Mitigated) Vulnerabilities

This section lists the vulnerabilities that were previously detected, then mitigated, and were re-detected in the latest scans. The table provides the initial detection and latest detection dates for each vulnerability.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	Backup Files Disclosure	Medium	x.x.51.172	443	2023-10-20 14:36	2024-02-02 19:12	105
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.74	443	2023-09-18 16:04	2024-02-03 13:19	137
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.108.76	443	2023-09-19 11:21	2024-02-04 04:10	137
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.49.143	443	2023-10-03 11:32	2024-02-03 03:32	122
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.137	443	2021-10-07 00:18	2024-02-03 13:23	849
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.77	8443	2021-10-06 16:20	2024-02-01 01:47	847
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.30	443	2018-06-29 08:27	2024-02-03 17:22	2045
SUB_ORG	SSL Certificate Expiry	Medium	x.x.49.143	443	2023-10-03 11:32	2024-02-03 03:32	122
SUB_ORG	SSL Certificate Expiry	Medium	x.x.80.30	443	2022-11-29 16:11	2024-02-03 17:22	431
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.59.77	8443	2021-10-06 16:20	2024-02-01 01:47	847
SUB_ORG	TLS Version 1.0 Protocol Detection	Medium	x.x.80.46	443	2021-10-06 23:13	2024-02-03 02:33	849
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.80.46	443	2022-04-07 19:37	2024-02-03 02:33	666
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.49.220	443	2023-11-24 05:46	2024-02-02 23:01	70
SUB_ORG	Web Application Potentially Vulnerable to Clickjacking	Medium	x.x.51.144	443	2023-08-16 07:24	2024-02-04 07:15	171

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	SSL Anonymous Cipher Suites Supported	Low	x.x.80.46	443	2021-10-06 23:13	2024-02-03 02:33	849
SUB_ORG	Web Server Allows Password Auto-Completion	Low	x.x.108.74	443	2023-09-18 16:04	2024-02-03 13:19	137
SUB_ORG	Web Server Allows Password Auto-Completion	Low	x.x.108.76	443	2023-09-19 11:21	2024-02-04 04:10	137
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.137	443	2021-10-07 00:18	2024-02-03 13:23	849
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.152	443	2021-10-06 16:42	2024-02-04 14:52	850

B.4 Recently-Detected Vulnerabilities

This section lists the vulnerabilities that were detected since the last report, but not detected in the latest scans. The table provides the initial detection and latest detection dates for each vulnerabilty. It is **strongly recommended** to verify if the vulnerabilities below were actively mitigated by your organization. If they were not, it is highly likely these vulnerabilities will be detected again by future scans.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	Age Days
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.152	443	2024-01-11 21:23	2024-01-29 11:27	17
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.18.151	443	2024-01-11 21:46	2024-01-29 10:00	17
SUB_ORG	Ivanti Connect Secure 9.x / 22.x Multiple Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)	Critical	x.x.20.200	443	2024-01-11 23:05	2024-01-29 10:41	17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	443	2021-10-06 19:20	2024-01-29 19:44	845
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.149	8883	2022-08-05 06:33	2024-01-29 19:44	542
SUB_ORG	SGDynamo sgdynamo.exe HTNAME Parameter Path Disclosure	Medium	x.x.50.49	443	2023-06-14 06:10	2024-01-29 21:46	229
SUB_ORG	Backup Files Disclosure	Medium	x.x.88.138	443	2023-09-08 02:12	2024-01-29 18:37	143
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.183	443	2023-12-19 13:36	2024-01-29 19:46	41
SUB_ORG	Web Server HTTP Header Internal IP Disclosure	Low	x.x.50.149	443	2021-10-06 19:20	2024-01-29 19:44	845

Appendix C Detailed Findings and Recommended Mitigations by Vulnerability

This section presents detailed scan results from the network mapping and vulnerability scans. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

Vulnerability	Severity	CVSS	Solution
Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	7.8	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
	3 Affected Host(s): x.x.18.151, x.x.18.152, x.x.20.200 *Initial Detection:* 2023-12-22 21:01 UTC *Latest Detection:* 2024-02-04 15:30 UTC *Description:* The Ivanti Connect Secure installed on the remote host is prior to 22.6R2. It is, therefore, affected by multiple vulnerabilities. - A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance. (CVE-2023-39340) - A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution. (CVE-2023-41719) - A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where a local attacker with access to an Ivanti Connect Secure (ICS) appliance can escalate their privileges by exploiting a vulnerable installed application. This vulnerability allows the attacker to gain elevated execution privileges on the affected system. (CVE-2023-41720) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.		
Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	7.5	Upgrade to Sun ONE Application Server 7.0 Update Release 1.
	1 Affected Host(s): x.x.58.57 *Initial Detection:* 2023-09-14 18:36 UTC *Latest Detection:* 2024-02-04 12:07 UTC *Description:* It is possible to make the remote web server disclose the source code of its JSP pages by requesting the pages with a different case (ie: filename.JSP instead of filename.jsp). An attacker may use this flaw to get the source code of your CGIs and possibly obtain passwords and other relevant information about this host.		

Vulnerability	Severity	CVSS	Solution
HSTS Missing From HTTPS Server (RFC 6797)	Medium	6.5	Configure the remote web server to use HSTS.

7 Affected Host(s): x.x.28.66, x.x.80.163, x.x.80.164, x.x.80.167, x.x.82.145, x.x.92.46, x.x.92.50
Initial Detection: 2021-03-14 20:11 UTC
Latest Detection: 2024-02-04 07:11 UTC
Description: The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Vulnerability	Severity	CVSS	Solution
SSL Certificate Cannot Be Trusted	Medium	6.5	Purchase or generate a proper SSL certificate for this service.

180 Affected Host(s): x.x.108.72, x.x.108.74, x.x.108.76, x.x.108.77, x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.103, x.x.49.111, x.x.49.127, x.x.49.128, x.x.49.13, x.x.49.143, x.x.49.144, x.x.49.146, x.x.49.188, x.x.49.195, x.x.49.196, x.x.49.218, x.x.49.247, x.x.49.248, x.x.49.85, x.x.49.86, x.x.50.110, x.x.50.111, x.x.50.137, x.x.50.152, x.x.50.155, x.x.50.158, x.x.50.16, x.x.50.17, x.x.50.18, x.x.50.188, x.x.50.21, x.x.50.218, x.x.50.24, x.x.50.252, x.x.50.253, x.x.50.32, x.x.51.1, x.x.51.13, x.x.51.134, x.x.51.135, x.x.51.138, x.x.51.139, x.x.51.14, x.x.51.143, x.x.51.155, x.x.51.160, x.x.51.162, x.x.51.173, x.x.51.175, x.x.51.176, x.x.51.177, x.x.51.184, x.x.51.221, x.x.51.236, x.x.51.24, x.x.51.31, x.x.51.32, x.x.51.38, x.x.51.39, x.x.51.40, x.x.51.42, x.x.51.55, x.x.51.69, x.x.52.125, x.x.52.144, x.x.52.145, x.x.52.193, x.x.52.194, x.x.52.214, x.x.52.218, x.x.57.105, x.x.57.106, x.x.57.108, x.x.57.122, x.x.57.123, x.x.57.13, x.x.57.138, x.x.57.139, x.x.57.141, x.x.57.188, x.x.57.221, x.x.57.222, x.x.57.225, x.x.57.235, x.x.57.74, x.x.57.89, x.x.57.90, x.x.58.101, x.x.58.102, x.x.58.11, x.x.58.143, x.x.58.146, x.x.58.15, x.x.58.179, x.x.58.202, x.x.58.203, x.x.58.21, x.x.58.225, x.x.58.232, x.x.58.240, x.x.58.241, x.x.58.242, x.x.58.248, x.x.58.249, x.x.58.25, x.x.58.250, x.x.58.251, x.x.58.55, x.x.58.6, x.x.58.7, x.x.58.72, x.x.59.12, x.x.59.13, x.x.59.15, x.x.59.32, x.x.59.38, x.x.59.43, x.x.59.54, x.x.59.61, x.x.59.63, x.x.59.68, x.x.59.69, x.x.59.73, x.x.59.74, x.x.59.75, x.x.59.76, x.x.59.77, x.x.59.79, x.x.59.81, x.x.59.88, x.x.60.12, x.x.60.128, x.x.60.129, x.x.60.13, x.x.60.138, x.x.60.157, x.x.60.158, x.x.60.161, x.x.60.162, x.x.60.163, x.x.60.167, x.x.60.168, x.x.60.193, x.x.60.198, x.x.60.199, x.x.60.207, x.x.60.224, x.x.60.225, x.x.60.228, x.x.60.230, x.x.60.231, x.x.60.232, x.x.60.34, x.x.80.186, x.x.80.234, x.x.80.30, x.x.80.33, x.x.80.57, x.x.84.145, x.x.85.159, x.x.85.160, x.x.85.166, x.x.87.21, x.x.87.3, x.x.87.4, x.x.89.129, x.x.91.187, x.x.91.188, x.x.92.152, x.x.92.171, x.x.92.249, x.x.93.2, x.x.95.15, x.x.95.32

Initial Detection: 2016-09-06 09:37 UTC

Latest Detection: 2024-02-04 17:29 UTC

Description: The server’s X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate’s ’notBefore’ dates, or after one of the certificate’s ’notAfter’ dates.

- Third, the certificate chain may contain a signature that either didn’t match the certificate’s information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate’s issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Vulnerability	Severity	CVSS	Solution
SSL Self-Signed Certificate	Medium	6.5	Purchase or generate a proper SSL certificate for this service.
			49 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.188, x.x.49.247, x.x.49.248, x.x.50.110, x.x.50.111, x.x.50.32, x.x.51.138, x.x.51.155, x.x.51.173, x.x.51.175, x.x.51.176, x.x.51.177, x.x.51.31, x.x.51.32, x.x.57.188, x.x.57.221, x.x.57.222, x.x.57.225, x.x.57.74, x.x.58.101, x.x.58.102, x.x.58.240, x.x.58.241, x.x.58.242, x.x.58.25, x.x.59.38, x.x.59.54, x.x.59.73, x.x.59.74, x.x.59.75, x.x.59.76, x.x.59.77, x.x.60.230, x.x.60.231, x.x.80.234, x.x.80.57, x.x.84.145, x.x.87.3, x.x.87.4, x.x.89.129, x.x.92.152, x.x.92.249, x.x.93.2 *Initial Detection:* 2020-04-05 17:21 UTC *Latest Detection:* 2024-02-04 16:32 UTC *Description:* The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.
TLS Version 1.0 Protocol Detection	Medium	6.5	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
			17 Affected Host(s): x.x.113.2, x.x.187.130, x.x.49.170, x.x.51.44, x.x.52.128, x.x.58.232, x.x.58.249, x.x.58.7, x.x.59.68, x.x.59.69, x.x.60.162, x.x.60.163, x.x.80.48, x.x.80.57, x.x.92.65, x.x.93.2, x.x.95.108 *Initial Detection:* 2020-04-02 00:42 UTC *Latest Detection:* 2024-02-04 17:06 UTC *Description:* The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that arenâ€™t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Vulnerability	Severity	CVSS	Solution
TLS Version 1.0 Protocol Detection	Medium	6.5	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.
			28 Affected Host(s): x.x.121.186, x.x.125.169, x.x.135.90, x.x.48.146, x.x.49.112, x.x.49.168, x.x.49.193, x.x.50.16, x.x.50.17, x.x.50.18, x.x.51.136, x.x.51.139, x.x.51.14, x.x.51.77, x.x.52.125, x.x.57.168, x.x.57.178, x.x.57.235, x.x.58.254, x.x.58.6, x.x.59.33, x.x.59.81, x.x.60.161, x.x.80.46, x.x.85.166, x.x.92.249, x.x.92.61, x.x.95.15 *Initial Detection:* 2020-04-02 05:14 UTC *Latest Detection:* 2024-02-04 16:23 UTC *Description:* The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
TLS Version 1.1 Protocol Deprecated	Medium	6.5	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
			76 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.168, x.x.49.170, x.x.49.174, x.x.49.193, x.x.49.195, x.x.49.196, x.x.49.233, x.x.50.16, x.x.50.17, x.x.50.18, x.x.50.253, x.x.51.134, x.x.51.135, x.x.51.136, x.x.51.139, x.x.51.14, x.x.51.143, x.x.51.144, x.x.51.172, x.x.51.208, x.x.51.229, x.x.51.230, x.x.51.38, x.x.51.39, x.x.51.40, x.x.51.42, x.x.51.44, x.x.51.69, x.x.51.77, x.x.52.125, x.x.57.168, x.x.57.178, x.x.57.238, x.x.58.203, x.x.58.232, x.x.58.248, x.x.58.249, x.x.58.250, x.x.58.251, x.x.58.254, x.x.58.6, x.x.58.7, x.x.59.12, x.x.59.127, x.x.59.13, x.x.59.32, x.x.59.33, x.x.59.43, x.x.59.68, x.x.59.69, x.x.59.72, x.x.59.79, x.x.59.81, x.x.60.161, x.x.60.162, x.x.60.163, x.x.60.198, x.x.80.46, x.x.80.48, x.x.82.145, x.x.88.161, x.x.91.209, x.x.91.248, x.x.91.250, x.x.91.251, x.x.92.249, x.x.92.61, x.x.92.65, x.x.93.2, x.x.95.108 *Initial Detection:* 2022-04-05 02:58 UTC *Latest Detection:* 2024-02-04 17:06 UTC *Description:* The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Vulnerability	Severity	CVSS	Solution
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	6.1	Upgrade to JQuery version 3.5.0 or later.
	4 Affected Host(s): x.x.109.211, x.x.50.155, x.x.58.143, x.x.83.87 *Initial Detection:* 2021-10-07 01:58 UTC *Latest Detection:* 2024-02-04 02:28 UTC *Description:* According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities. Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.		
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	5.9	Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.
	11 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.182, x.x.51.235, x.x.57.182, x.x.92.249, x.x.93.2 *Initial Detection:* 2023-12-28 03:12 UTC *Latest Detection:* 2024-02-04 14:44 UTC *Description:* The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security. Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.		
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	5.9	Contact the Certificate Authority to have the SSL certificate reissued.
	9 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.80.161, x.x.92.249, x.x.93.2 *Initial Detection:* 2022-06-22 01:24 UTC *Latest Detection:* 2024-02-04 09:36 UTC *Description:* The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.		

Vulnerability	Severity	CVSS	Solution
Apache Tomcat Default Files	Medium	5.3	Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.
			2 Affected Host(s): x.x.51.135, x.x.59.13 *Initial Detection:* 2021-10-06 04:01 UTC *Latest Detection:* 2024-02-02 21:12 UTC *Description:* The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.
IIS Detailed Error Information Disclosure	Medium	5.3	Configure the IIS server to deliver custom rather than detailed error messages.
			3 Affected Host(s): x.x.50.47, x.x.58.40, x.x.58.42 *Initial Detection:* 2023-06-24 13:24 UTC *Latest Detection:* 2024-02-04 16:34 UTC *Description:* The remote Microsoft IIS web server is improperly configured to deliver detailed error messages. These detailed error messages may contain confidential diagnostic information, such as the file system paths to hosted content and logon information.
OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	5.3	Upgrade to OpenSSL version 1.1.1x or later.
			8 Affected Host(s): x.x.50.110, x.x.50.111, x.x.52.176, x.x.52.177, x.x.58.101, x.x.58.102, x.x.60.195, x.x.60.196 *Initial Detection:* 2023-11-08 00:17 UTC *Latest Detection:* 2024-02-04 04:34 UTC *Description:* The version of OpenSSL installed on the remote host is prior to 1.1.1x. It is, therefore, affected by a vulnerability as referenced in the 1.1.1x advisory. - Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the -pubcheck option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678) Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Item 9.

Vulnerability	Severity	CVSS	Solution
SSL Certificate Expiry	Medium	5.3	Purchase or generate a new SSL certificate to replace the existing one.
	43 Affected Host(s): x.x.113.2, x.x.121.186, x.x.125.169, x.x.135.90, x.x.187.130, x.x.48.146, x.x.49.143, x.x.49.144, x.x.51.13, x.x.51.134, x.x.51.135, x.x.51.143, x.x.51.38, x.x.51.39, x.x.51.40, x.x.51.42, x.x.52.125, x.x.57.108, x.x.57.138, x.x.57.139, x.x.57.74, x.x.58.203, x.x.58.21, x.x.58.248, x.x.58.249, x.x.58.250, x.x.58.251, x.x.58.72, x.x.59.12, x.x.59.13, x.x.59.15, x.x.59.43, x.x.59.68, x.x.59.69, x.x.60.138, x.x.60.161, x.x.60.162, x.x.60.163, x.x.80.30, x.x.80.57, x.x.92.171, x.x.92.249, x.x.93.2 *Initial Detection:* 2021-10-06 06:33 UTC *Latest Detection:* 2024-02-04 17:06 UTC *Description:* This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.		
Backup Files Disclosure	Medium	5.0	Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.
	7 Affected Host(s): x.x.51.172, x.x.57.105, x.x.57.129, x.x.57.140, x.x.57.141, x.x.59.72, x.x.85.185 *Initial Detection:* 2022-05-04 17:21 UTC *Latest Detection:* 2024-02-04 16:41 UTC *Description:* By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.		
F5 BIG-IP Cookie Remote Information Disclosure	Medium	5.0	Contact the vendor for a fix.
	2 Affected Host(s): x.x.80.172, x.x.83.87 *Initial Detection:* 2023-09-11 10:27 UTC *Latest Detection:* 2024-02-04 03:44 UTC *Description:* The remote host appears to be an F5 BIG-IP load balancer. The load balancer encodes the IP address of the actual web server that it is acting on behalf of within a cookie. Additionally, information after ’BIGipServer’ is configured by the user and may be the logical name of the device. These values may disclose sensitive information, such as internal IP addresses and names.		
Multiple Web Server Encoded Space (%20) Request ASP Source Disclosure	Medium	5.0	There is no known solution at this time.
	2 Affected Host(s): x.x.50.68, x.x.58.57 *Initial Detection:* 2023-09-08 01:14 UTC *Latest Detection:* 2024-02-04 12:07 UTC *Description:* It appears possible to get the source code of the remote ASP scripts by appending a ’%20’ to the request. ASP source code usually contains sensitive information such as logins and passwords. This has been reported in Simple HTTPD (shttpd), Mono XSP for ASP.NET and vWebServer. This type of request may affect other web servers as well.		

Vulnerability	Severity	CVSS	Solution
Nonexistent Page (404) Physical Path Disclosure	Medium	5.0	Upgrade the web server to the latest version. Alternatively, reconfigure the web server to disable debug reporting.
	1 Affected Host(s): x.x.50.49 *Initial Detection:* 2023-06-26 14:26 UTC *Latest Detection:* 2024-02-03 02:56 UTC *Description:* The remote web server reveals the physical path of the webroot when a nonexistent page is requested. While printing errors to the output is useful for debugging applications, this feature should be disabled on production servers.		
Sun ONE Application Server Upper Case Request JSP Source Disclosure	Medium	5.0	Upgrade to Sun ONE Application Server 7.0 Update Release 1.
	1 Affected Host(s): x.x.50.68 *Initial Detection:* 2023-09-08 01:14 UTC *Latest Detection:* 2024-02-01 03:22 UTC *Description:* It is possible to make the remote web server disclose the source code of its JSP pages by requesting the pages with a different case (ie: filename.JSP instead of filename.jsp). An attacker may use this flaw to get the source code of your CGIs and possibly obtain passwords and other relevant information about this host.		
HTTP TRACE / TRACK Methods Allowed	Medium	4.3	Disable these HTTP methods. Refer to the plugin output for more information.
	10 Affected Host(s): x.x.109.141, x.x.109.142, x.x.109.143, x.x.109.181, x.x.109.205, x.x.52.176, x.x.52.177, x.x.60.195, x.x.60.196, x.x.60.41 *Initial Detection:* 2017-08-30 17:29 UTC *Latest Detection:* 2024-02-04 04:17 UTC *Description:* The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.		
SSH Weak Algorithms Supported	Medium	4.3	Contact the vendor or consult product documentation to remove the weak ciphers.
	2 Affected Host(s): x.x.49.182, x.x.57.182 *Initial Detection:* 2021-10-06 13:13 UTC *Latest Detection:* 2024-02-04 14:44 UTC *Description:* Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.		

Vulnerability	Severity	CVSS	Solution
Web Application Potentially Vulnerable to Clickjacking	Medium	4.3	Return the X-Frame-Options or Content-Security-Policy (with the ’frame-ancestors’ directive) HTTP header with the page’s response. This prevents the page’s content from being rendered by another site when using the frame or iframe HTML tags.

3 Affected Host(s): x.x.49.220, x.x.51.144, x.x.59.44

Initial Detection: 2023-08-16 07:24 UTC

Latest Detection: 2024-02-04 07:15 UTC

Description: The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy ’frame-ancestors’ response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The ’frame-ancestors’ policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

<table>
<tr><th>Vulnerability</th><th>Severity</th><th>CVSS</th><th>Solution</th></tr>
<tr><td>SSH Weak Key Exchange Algorithms Enabled</td><td>Low</td><td>3.7</td><td>Contact the vendor or consult product documentation to disable the weak algorithms.</td></tr>
<tr><td></td><td colspan="3"><i><u>7 Affected Host(s):</u></i> x.x.131.161, x.x.207.145, x.x.58.228, x.x.58.229, x.x.6.41, x.x.60.201, x.x.83.74
<i><u>Initial Detection:</u></i> 2021-10-14 16:24 UTC
<i><u>Latest Detection:</u></i> 2024-02-03 03:36 UTC
<i><u>Description:</u></i> The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.</td></tr>
<tr><td>SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)</td><td>Low</td><td>3.7</td><td>Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.</td></tr>
<tr><td></td><td colspan="3"><i><u>2 Affected Host(s):</u></i> x.x.50.17, x.x.58.7
<i><u>Initial Detection:</u></i> 2021-11-12 17:26 UTC
<i><u>Latest Detection:</u></i> 2024-02-04 04:04 UTC
<i><u>Description:</u></i> The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.</td></tr>
</table>

Vulnerability	Severity	CVSS	Solution
SSH Server CBC Mode Ciphers Enabled	Low	2.6	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
	6 Affected Host(s): x.x.49.182, x.x.57.182, x.x.58.228, x.x.58.229, x.x.6.41, x.x.83.74 *Initial Detection:* 2016-04-26 15:35 UTC *Latest Detection:* 2024-02-04 14:44 UTC *Description:* The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.		
SSH Weak MAC Algorithms Enabled	Low	2.6	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
	7 Affected Host(s): x.x.131.161, x.x.207.145, x.x.58.228, x.x.58.229, x.x.6.41, x.x.60.201, x.x.83.74 *Initial Detection:* 2020-02-05 17:41 UTC *Latest Detection:* 2024-02-03 03:36 UTC *Description:* The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.		
SSL Anonymous Cipher Suites Supported	Low	2.6	Reconfigure the affected application if possible to avoid use of weak ciphers.
	3 Affected Host(s): x.x.51.77, x.x.80.46, x.x.80.48 *Initial Detection:* 2021-10-05 21:24 UTC *Latest Detection:* 2024-02-04 00:11 UTC *Description:* The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack. Note: This is considerably easier to exploit if the attacker is on the same physical network.		
Web Server HTTP Header Internal IP Disclosure	Low	2.6	Apply configuration suggested by vendor.
	18 Affected Host(s): x.x.109.146, x.x.49.111, x.x.49.112, x.x.49.134, x.x.49.135, x.x.49.136, x.x.50.137, x.x.50.152, x.x.52.182, x.x.57.105, x.x.57.106, x.x.57.107, x.x.57.129, x.x.57.130, x.x.57.131, x.x.58.66, x.x.82.145, x.x.87.227 *Initial Detection:* 2019-03-31 17:57 UTC *Latest Detection:* 2024-02-04 17:28 UTC *Description:* This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection.		

Vulnerability	Severity	CVSS	Solution
Web Server Load Balancer Detection	Low	2.6	Update the web configuration to hide information disclosure.
	3 Affected Host(s): x.x.52.182, x.x.82.145, x.x.87.227 *Initial Detection:* 2020-01-24 05:52 UTC *Latest Detection:* 2024-02-03 03:54 UTC *Description:* The remote web server seems to be running in conjunction with several others behind a load balancer. Knowing that there are multiple systems behind a service could be useful to an attacker as the underlying hosts may be running different operating systems, patchlevels, etc.		
Web Server Allows Password Auto-Completion	Low	0.0	Add the attribute ’autocomplete=off’ to these fields to prevent browsers from caching credentials.
	5 Affected Host(s): x.x.108.72, x.x.108.74, x.x.108.76, x.x.108.77, x.x.64.167 *Initial Detection:* 2023-07-22 11:12 UTC *Latest Detection:* 2024-02-04 08:09 UTC *Description:* The remote web server contains at least one HTML form field that has an input of type ’password’ where ’autocomplete’ is not set to ’off’. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.		

Appendix D Critical and High Vulnerability Mitigations by IP Address

This section presents detailed scan results, ordered by host, from the network mapping and vulnerability scans. The table only displays high and critical vulnerabilities. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

Owner	Host	Port(s)	Vulnerability	Severity	Age Days	Solution
SUB_ORG	x.x.18.151	443	Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	42	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
SUB_ORG	x.x.18.152	443	Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	43	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
SUB_ORG	x.x.20.200	443	Ivanti Connect Secure < 22.6R2 Multiple Vulnerabilities	High	42	Upgrade to Ivanti Secure Desktop Client 22.6R2 or later.
SUB_ORG	x.x.58.57	443	Sun ONE Application Server Upper Case Request JSP Source Disclosure	High	142	Upgrade to Sun ONE Application Server 7.0 Update Release 1.

Appendix E False Positive Findings

This section lists findings that SAMPLE asserted to CISA to be false positives (i.e., data that incorrectly indicates a vulnerability is present). If SAMPLE would like to report findings for false positive consideration, please complete the False Positive Assertion Form included in Appendix G: Attachments. Unless CISA determines the submission is insufficient, CISA will leave the determination for what constitutes a false positive to report recipients. False positive status expires by default 365 days after the false positive was marked as such by CISA. When a finding's false positive status expires, the finding will be removed from this section. If the finding is then re-detected, CISA recommends SAMPLE review its status.

E.1 Expiring Soon False Positive Findings

This section lists false positive findings whose status as a false positive is expiring within 30 days. If SAMPLE would like to extend the expiration date of a false positive, please submit an email through your designated technical point of contact with an analysis and evidence indicating how SAMPLE determined the finding is still considered a false positive. For a full listing of false positives, please see Appendix E.2: All False Positive Findings.

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.43	443	2021-10-07 04:16	2024-01-14 05:08	2023-10-20	2024-02-20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.252	443	2022-02-09 06:14	2024-01-13 23:16	2023-10-20	2024-02-20
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.51.43	443	2022-04-07 03:04	2024-01-14 05:08	2023-11-27	2024-02-20
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.58.252	443	2023-01-29 08:31	2024-01-13 23:16	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.83.72	443	2023-01-30 09:56	2023-11-25 20:32	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.51.43	443	2023-01-30 10:25	2024-01-14 05:08	2023-03-03	2024-03-02
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.160.139	443	2023-02-14 21:41	2024-02-04 04:01	2023-06-01	2024-03-04

E.2 All False Positive Findings

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.43	443	2021-10-07 04:16	2024-01-14 05:08	2023-10-20	2024-02-20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.252	443	2022-02-09 06:14	2024-01-13 23:16	2023-10-20	2024-02-20
SUB_ORG	TLS Version 1.1 Protocol Deprecated	Medium	x.x.51.43	443	2022-04-07 03:04	2024-01-14 05:08	2023-11-27	2024-02-20
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.58.252	443	2023-01-29 08:31	2024-01-13 23:16	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.83.72	443	2023-01-30 09:56	2023-11-25 20:32	2023-03-03	2024-03-02
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.51.43	443	2023-01-30 10:25	2024-01-14 05:08	2023-03-03	2024-03-02
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.160.139	443	2023-02-14 21:41	2024-02-04 04:01	2023-06-01	2024-03-04
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.162	443	2023-02-21 21:00	2024-02-04 03:58	2023-06-28	2024-03-18
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	443	2016-09-02 14:25	2024-02-04 04:22	2023-04-07	2024-04-06

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	443	2016-09-02 14:25	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	10443	2019-03-28 15:16	2024-02-04 04:22	2023-10-09	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	10443	2019-03-28 15:16	2024-02-04 04:22	2023-10-09	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	10443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	10443	2021-10-06 05:03	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.52	443	2021-10-07 05:03	2024-02-04 17:13	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	643	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	643	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	1443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	1443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	7443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	7443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	6443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	6443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.150	4443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.150	4443	2022-08-05 14:14	2024-02-04 04:22	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	7443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	7443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	1443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	1443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	6443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	6443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	643	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	643	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.137	4443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.137	4443	2022-08-07 15:44	2024-02-02 19:21	2023-04-07	2024-04-06
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.18.152	443	2020-04-10 11:14	2024-02-04 15:30	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.18.152	443	2020-04-10 11:14	2024-02-04 15:30	2023-07-05	2024-04-10
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.18.151	443	2020-04-10 11:18	2024-02-04 11:09	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.18.151	443	2020-04-10 11:18	2024-02-04 11:09	2023-07-05	2024-04-10
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.20.200	443	2020-04-10 11:22	2024-02-04 11:15	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.20.200	443	2020-04-10 11:22	2024-02-04 11:15	2023-07-05	2024-04-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.0	443	2021-10-05 23:32	2024-02-02 17:46	2023-09-27	2024-05-17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.224	443	2021-10-06 18:11	2024-02-04 03:27	2023-09-27	2024-05-17
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.11	443	2021-10-06 10:02	2024-02-03 23:40	2023-09-27	2024-05-19
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.20	443	2021-10-06 20:42	2024-02-04 04:31	2023-09-20	2024-05-19
SUB_ORG	SSL Certificate Expiry	Medium	x.x.51.11	443	2023-05-11 22:46	2024-02-03 23:40	2023-09-27	2024-05-19

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.41	443	2023-06-07 17:04	2024-02-04 04:37	2023-07-14	2024-06-08
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.9.44	443	2021-07-09 15:34	2024-01-25 03:11	2023-06-15	2024-06-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.9.44	443	2021-07-09 15:34	2024-01-25 03:11	2023-06-15	2024-06-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.203.203	443	2021-07-09 15:34	2024-02-02 17:37	2023-07-10	2024-06-20
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.161	443	2022-06-08 10:03	2024-02-03 02:00	2023-06-30	2024-06-29
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.161	443	2022-08-29 09:37	2024-02-03 02:00	2023-06-30	2024-06-29
SUB_ORG	Backup Files Disclosure	Medium	x.x.85.123	443	2023-08-10 18:10	2024-02-04 01:33	2024-01-11	2024-06-30
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.88.138	443	2023-09-12 06:52	2024-02-03 00:22	2023-09-20	2024-06-30
SUB_ORG	TLS Version 1.0 Protocol Detection	High	x.x.85.123	443	2018-07-01 20:13	2023-11-11 23:58	2023-11-11	2024-07-01
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.123	443	2023-06-14 11:26	2024-02-04 01:33	2023-07-06	2024-07-05
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.186.112	443	2023-06-17 03:50	2024-02-03 01:50	2023-07-06	2024-07-05
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.160	443	2023-06-15 15:28	2024-02-04 05:04	2024-01-19	2024-07-06
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.158	443	2023-06-29 06:19	2024-02-02 21:40	2023-09-27	2024-07-23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.157	443	2023-06-30 20:34	2024-02-02 17:56	2023-09-27	2024-07-23
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.232	443	2012-11-27 10:21	2024-02-03 00:08	2023-07-26	2024-07-25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.232	443	2017-06-08 02:25	2024-02-03 00:08	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.89.152	443	2018-09-09 19:47	2024-02-03 01:48	2023-07-26	2024-07-25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.89.152	443	2018-09-09 19:47	2024-02-03 01:48	2023-07-26	2024-07-25
SUB_ORG	SSL Self-Signed Certificate	Medium	x.x.80.233	443	2021-10-05 23:51	2024-02-03 22:30	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.233	443	2021-10-05 23:51	2024-02-03 22:30	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.89.153	443	2021-10-07 01:59	2024-02-04 04:20	2023-07-26	2024-07-25
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.159	443	2023-03-16 23:07	2024-02-04 05:17	2023-09-27	2024-08-03
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.177	443	2023-07-25 01:01	2024-01-28 01:39	2023-08-04	2024-08-03
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.216	443	2023-07-27 12:43	2024-02-04 02:29	2023-08-04	2024-08-03
SUB_ORG	Drupal PHPUnit/Mailchimp Code Execution Vulnerability	Critical	x.x.58.55	443	2023-07-22 18:55	2023-10-04 15:11	2023-08-07	2024-08-06
SUB_ORG	Spring Framework Spring4Shell (CVE-2022-22965)	Critical	x.x.80.53	443	2022-04-12 01:16	2023-12-09 17:43	2023-08-11	2024-08-10
SUB_ORG	Spring Framework Spring4Shell (CVE-2022-22965)	Critical	x.x.165.41	443	2022-04-13 07:50	2023-12-09 11:54	2023-08-11	2024-08-10
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.141	8083	2023-08-02 15:56	2024-02-03 03:20	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	8443	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	8444	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	10002	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	8081	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.11.140	20000	2023-08-02 16:22	2024-02-03 00:22	2023-08-15	2024-08-14
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.30	443	2016-09-02 14:25	2024-02-03 01:52	2023-09-20	2024-08-15
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.10	443	2021-10-13 14:47	2024-02-04 01:17	2023-09-20	2024-09-01
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.172	443	2022-06-26 11:30	2024-02-04 03:44	2023-09-22	2024-09-21

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.49.231	443	2023-05-19 17:33	2024-02-04 04:30	2023-10-16	2024-10-15
SUB_ORG	TLS Version 1.0 Protocol Detection	Medium	x.x.49.231	443	2023-07-10 15:50	2024-02-04 04:30	2023-10-16	2024-10-15
SUB_ORG	Backup Files Disclosure	Medium	x.x.57.150	443	2023-10-25 12:48	2024-02-03 01:20	2023-12-05	2024-11-03
SUB_ORG	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Critical	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Critical	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1o Vulnerability	Critical	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1p Vulnerability	Critical	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1l Vulnerability	High	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1n Vulnerability	High	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities	High	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1l Vulnerability	High	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1n Vulnerability	High	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities	High	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.58.17	443	2023-08-23 16:32	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.50.26	443	2023-08-23 22:53	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1m Vulnerability	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1q Vulnerability	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1v Vulnerability	Medium	x.x.58.17	443	2023-10-06 15:07	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1m Vulnerability	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1q Vulnerability	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1v Vulnerability	Medium	x.x.50.26	443	2023-10-06 17:41	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Medium	x.x.58.17	443	2023-10-19 22:09	2023-11-28 00:45	2023-11-14	2024-11-13
SUB_ORG	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Medium	x.x.50.26	443	2023-10-19 22:18	2023-11-28 00:52	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	x.x.50.26	443	2023-11-07 23:40	2024-02-04 08:54	2023-11-14	2024-11-13
SUB_ORG	OpenSSL 1.1.1 < 1.1.1x Vulnerability	Medium	x.x.58.17	443	2023-11-08 00:35	2024-02-04 03:23	2023-11-14	2024-11-13
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.125.62	443	2023-12-13 10:13	2024-01-31 22:31	2023-12-21	2024-12-03
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.32	443	2022-10-01 00:13	2024-02-04 00:44	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.234	443	2022-10-01 12:17	2024-02-02 21:56	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.234	49443	2022-10-01 12:17	2024-02-02 21:56	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.231	49443	2022-10-01 12:32	2024-02-02 21:12	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.231	443	2022-10-01 12:32	2024-02-02 21:12	2023-12-08	2024-12-07

Owner	Vulnerability	Severity	Host	Port	Initial Detection (UTC)	Latest Detection (UTC)	False Positive Effective	False Positive Expiration
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.232	443	2022-10-09 09:36	2024-02-03 01:37	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.232	49443	2022-10-09 09:36	2024-02-03 01:37	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.233	49443	2022-10-09 09:54	2024-02-03 02:07	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.233	443	2022-10-09 09:54	2024-02-03 02:07	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.31	443	2022-10-09 11:29	2024-02-03 02:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.87	443	2023-03-30 11:25	2024-02-04 00:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.182	443	2023-03-30 17:35	2024-02-04 00:30	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.51.182	49443	2023-05-11 23:00	2024-02-04 00:30	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.166	443	2023-06-22 09:50	2024-02-02 19:14	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.59.87	49443	2023-08-11 15:15	2024-02-04 00:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.80.167	443	2023-08-23 09:17	2024-02-04 07:11	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.32	49443	2023-09-07 13:19	2024-02-04 00:44	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.60.31	49443	2023-09-08 22:32	2024-02-03 02:27	2023-12-08	2024-12-07
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.95.28	443	2023-06-19 21:51	2024-02-04 04:44	2024-01-25	2025-01-24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.85.164	443	2023-09-23 00:29	2024-02-04 03:02	2024-01-25	2025-01-24
SUB_ORG	SSL Certificate Cannot Be Trusted	Medium	x.x.87.28	443	2023-09-27 16:43	2024-02-04 05:24	2024-01-25	2025-01-24

Appendix F Frequently Asked Questions

This section seeks to answer the most frequently asked questions about Cyber Hygiene reports.

1. **I think the vulnerability listed in my report is a false positive. Can you remove it from my report?**
   - If you believe a finding to be in error, please complete and return the False Positive Assertion Form found in Appendix G: Attachments to CISA.
   - CISA will review and perform our own analysis. This will not include exploiting a vulnerability, but may include actively sending packets to the host in question.
   - If our research appears to confirm your analysis, the vulnerability will be marked as a false positive for that host and will stop appearing in the main body of the report for one year. Vulnerabilities marked as ’false positive’ will be reported in Appendix E: False Positive Findings, along with the dates of when the false positive took effect and when it will expire.
   - CISA reserves the right to assert that certain findings are not false positives, and when false positive assertions are accepted by CISA, that acceptance should not be construed as validation that a finding is in fact a false positive.
2. **Can I get the data you created this report from in CSV?**
   - Certainly! See Appendix G: Attachments.
3. **I fixed a vulnerability listed in my report. Can you rescan to verify?**
   - CyHy automatically rescans whenever a vulnerability is detected, so there is no need to notify us that you’ve fixed something. If we can no longer detect the vulnerability, it will be listed in Appendix B.1: Mitigated Vulnerabilities.
4. **The CISA Binding Operational Directive 15-01 (BOD) requires my agency to fix Critical vulnerabilities within 30 days. If we can’t do that, who do we contact and what needs to be sent?**
   - For all questions or submissions related to the BOD, please email fnr.bod@hq.dhs.gov.
   - To be clear, if a Critical vulnerability
     - is less than 30 days old and your agency can fix it before it hits 30 days old, nothing needs to be sent to CISA.
     - can’t or won’t be fixed within 30 days (or it’s already older than 30 days), send fnr.bod@hq.dhs.gov a Plan Of Action and Milestones (POA&M) that includes the following information:
       (a) a detailed justification outlining any barriers to expedited mitigation,
       (b) the steps you are taking to get to a resolution, and
       (c) a timeframe for mitigation.
   - Remediation of the Critical vulnerability will be validated when our scans no longer detect the vulnerability, not through an assessment of or concurrence with your submitted POA&M. Even with the submission of a POA&M, the vulnerability will continue to be listed on your CyHy report until remediated (i.e., it will not be marked as a false positive).
5. **Can I add my third-party hosted/managed servers?**
   - Yes, and we recommend that you do so, but we request that you obtain authorization/consent before we begin scanning them. CISA does not require documentation from your third-parties.
6. **Why do the host counts in my Cyber Hygiene report not match the number of known Internet-facing end points on my network?**
   - This is likely due to a difference in what we’re defining as a host. CyHy considers a device a host if there is at least one open port/service operating at the address. When we scan, any number of things can occur that make it appear that nothing is at that address (e.g., our scans are blocked by host or network filters, the device is down for maintenance, packets are dropped or lost en route, etc.).
   - If a port is detected as ’tcpwrapped’, it means that the TCP handshake was completed, but the connection was closed before any data was sent back. For the purposes of this report, tcpwrapped ports are not considered to be ’open’. If a device only responds with tcpwrapped ports, then it will not be considered a host by CyHy. For more information about tcpwrapped ports, see https://secwiki.org/w/FAQ_tcpwrapped.

- The intent of CyHy is to find vulnerabilities, not count hosts, and our metrics should not be relied upon as a verified host count of your organization. The weekly host count should be taken as an estimate. If, however, there are no or extremely low host counts reported when there are known active hosts, it is possible that the CyHy scans are being blocked.

7. **I've added a new host and your scans are not picking it up.**

    - CyHy is not scanning your entire IP scope every week. If you've stood up a new server in a range that we only recently scanned and found nothing in, it's possible that the new server would not appear for nearly 90 days. If you want the new host to be scanned immediately, you can email vulnerability@cisa.dhs.gov and we'll manually scan it, which will add it to your weekly report.

8. **I'm getting SSL/TLS certificate vulnerabilities that I think are incorrect.**

    - In our scans, we will use the Mozilla trust store. CISA will not accept any other roots. This is done as a matter of practice and principle: as practice, because maintaining private roots from our various stakeholders is operationally infeasible; as principle, because our scans aim to ensure that the user of your services is protected. The Mozilla trust store is generally representative of a 'lowest common denominator' in what a public-serving site can reasonably expect of those users whose devices they do not manage.
    - Ensure that the root your certificate is issued from is included in the Mozilla root store. You should also verify that the intermediate certificates are presented with your site certificate. This allows the scanner to validate the certificate's chain of trust.
    - Though the site is Federal Government-centric, tons of great information can be found at https.cio.gov regarding Hypertext Transfer Protocol Secure (HTTPS), much of which is applicable for SSL/TLS more generally.

9. **What do the different appendices represent? How can a vulnerability be in more than one appendix? Which vulnerabilities are counted in the Report Card?**

Vulnerability Type	Counted in Report Card?	Listed in Appendix A	B.1	B.2	B.3	B.4	C
Detected in latest scan, for the first time (i.e. "brand new vulnerability")	Yes	✓		✓			✓
Re-detected in latest scan (previously reported; was present in last week's Appendix A and C)	Yes	✓					✓
Re-detected in latest scan (previously reported and mitigated; was NOT present in last week's Appendix A and C)	Yes	✓			✓		✓
Reported last week in Appendix A and C, but not detected since then (i.e. "currently mitigated")	No		✓				
Not detected in latest scan, but detected at some point between last report and latest scan	No					✓	

10. **Can you scan my IPv6 addresses?**

    - There is currently no ETA for CyHy to scan IPv6 addresses.

11. **Can you scan this list of domains for me?**

    - For vulnerability scanning, CyHy does not presently scan domain names directly, however, we are looking into adding this feature in the future.

12. **How can I change who receives my Cyber Hygiene report?**

    - The CyHy report will be delivered to a single address. Most organizations set up a distribution address which takes incoming mail and delivers it to individual mailboxes. CISA strongly recommends this approach because it allows your organization to grant access to the report to whomever you'd like, as well as manage the change control of employees onboarding or leaving. If you need to change the distro we mail to, email us at vulnerability@cisa.dhs.gov.

13. **Can I change the password for my report?**

    - If you need to request a new password for your report, email us at vulnerability@cisa.dhs.gov. Please let us know if you'd like the password texted, delivered over the phone (note if voicemail is ok), or just emailed back.

14. **How is the age of each vulnerability calculated?**

    - Vulnerability age is determined by when it was first detected on a host, not from when it first appeared on a report. For more information, refer to the “Recurring Vulnerabilities” paragraph in Section 8.2: Methodology / Process.

15. **I own a 2nd-level domain that is not represented in my certificate data.**

    - If you believe we are missing 2nd-level domains, you can reach out to vulnerability@cisa.dhs.gov and request that we add them to our domain gatherer.

Item 9.

Appendix G Attachments

If your PDF viewer supports embedded attachments you will see paper clip icons below for each attached file which includes additional report details. To access the attachments embedded within the report, open the report with a dedicated PDF reader (such as Adobe Acrobat), and click on the paper clip icon to the left of the attachment name.

- certificates.csv : Data collected about each certificate found that was issued for a domain known to belong to you.
- cyber-hygiene-data-sharing-form.pdf: Form to request your weekly findings be shared with a trusted third party (e.g. MSP, ISAC, Consultant, etc.); send the completed form to vulnerability@cisa.dhs.gov.
- cyber-hygiene-false-positive-assertion-form.pdf: Form to request that one or more vulnerabilities be marked as false positives; send the completed form to vulnerability@cisa.dhs.gov.
- days-currently-active.csv: Metrics over time for median and maximum age of active vulnerabilities (active as of date listed in each row).
- days-to-mitigate.csv: Metrics over time for median and maximum days to mitigate findings (calculated with vulnerabilities mitigated since date listed in each row).
- domains.csv : A CSV containing all the base domains we know belong to you.
- false-positive-findings.csv : List of all reported false positive vulnerability findings.
- findings.csv : Detailed list of all vulnerability findings for each IP address and port.
- hosts.csv : List of hosts discovered with IP address, best-guess OS identification, and hostname if available.
- mitigated-vulnerabilities.csv : List of vulnerabilities that were included on the last report, but were not detected in the latest scans.
- potentially-risky-services.csv : List of all potentially risky services detected and the associated IP address and port.
- recently-detected.csv : List of all vulnerabilities detected since the last report, but not detected in the latest scans.
- scope.csv : List of IP addresses that were in scope for this report.
- services.csv : List of all discovered services and the associated IP address and port. NOTE: This attachment excludes the 1,986,714 service(s) detected as ’tcpwrapped’, which indicates that a full TCP handshake was completed, but the connection was closed before any data was sent. For more information, refer to the Frequently Asked Questions section.
- sub-org-summary.csv : Data from the Sub-Organization Summary.

Appendix H Glossary and Acronyms

Glossary

active vulnerability A vulnerability that was detected in the most recent scan of a host used for this report. 11, 18

false positive Any normal or expected behavior that is identified in this report as a potentially exploitable vulnerability. 10, 18, 42, 47, 50

host A device that has a least one open port/listening service. 5, 10, 14, 15, 17–19, 22, 41, 47, 50

host scan A scan of all assets to identify hosts. 6

initial detection The initial point in time when Cyber Hygiene scans identified a vulnerability. This date is used to calculate the vulnerability's age. 11, 12, 15, 25–27

known exploited vulnerability A vulnerability listed in CISA's catalog of known exploited vulnerabilities. For more information, please refer to Section 3: Binding Operational Directive 22-01 — Reducing the Significant Risk of Known Exploited Vulnerabilities. 7

latest detection The most recent time when Cyber Hygiene scans identified a particular vulnerability. 26, 27

mitigation detection The date when a previously identified vulnerability was no longer detected by Cyber Hygiene scans. 25

service An application running at the network application layer that provides communications capabilities across an IP computer network. 5, 14, 15, 21, 50

severity Please review the following guide for vulnerability severity scoring information: https://www.first.org/cvss/v2/guide. 5, 15, 19, 22, 24

vulnerability A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. 5, 7, 10–12, 14, 15, 18, 19, 21–28, 41, 42, 47, 50

vulnerability age The time between a vulnerability's initial detection date and its latest detection date. 11, 12, 15, 49

vulnerability scan A vulnerability scan on all hosts identified during host scan. 6

vulnerable host A host with at least one vulnerability detected on the most recent scan used for this report. 22

Acronyms

AWS Amazon Web Services. 14

CIRCIA Cyber Incident Reporting for Critical Infrastructure Act of 2022. 7

CISA Cybersecurity and Infrastructure Security Agency [https://www.cisa.gov]. 5, 7–10, 14, 15, 18, 23, 42, 47, 48

CSV Comma-Separated Values. 5, 13, 14, 47, 50

CT Certificate transparency. 9

CVE Common Vulnerabilities and Exposures; for more information refer to https://cve.mitre.org/about/faqs.html. 7, 16

CVSS Common Vulnerability Scoring System; for more information refer to https://www.first.org/cvss/v2. 4, 16, 18, 19

CyHy Cyber Hygiene. 5, 10–14, 16, 18, 20, 47, 48

DNS Domain Name Service. 9

HTTPS Hypertext Transfer Protocol Secure. 48

IP Internet Protocol. 14, 48, 50

IT Information Technology. 10

KEV Known Exploited Vulnerability. 7

NVD National Vulnerability Database; for more information refer to https://nvd.nist.gov. 16

OS Operating System. 14, 50

POA&M Plan Of Action and Milestones. 47

RRS Risk Rating System. 19

RVWP Ransomware Vulnerability Warning Pilot. 7

SAMPLE Sample Organization. 5, 10–14, 17, 18, 21–23, 42

TCP Transmission Control Protocol. 14, 50

Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

MS-ISAC Services Guide

Contents

MS-ISAC Services Guide

MS-ISAC Overview

The Multi-State Information Sharing and Analysis Center® (MS-ISAC®), has been designated by the Cybersecurity & Infrastructure Security Agency (CISA) as the key resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments.

The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, and increased communication.

The MS-ISAC is a division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit. Visit **cisecurity.org/ms-isac/** or **info@cisecurity.org** for more information.

JOINING THE MS-ISAC

There is no cost to join the MS-ISAC, and membership is open to all SLTT government entities. The only requirement is agreement to the Terms and Conditions, which outlines a member's responsibilities to protect information that is shared.

What We Offer

- The MS-ISAC provides **real-time** network monitoring and management, threat analysis, and early warning notifications through the 24×7×365 Security Operations Center (SOC).
- Focal point for cyber threat prevention, protection, response and recovery for U.S. SLTT governments.
- We perform **incident response and remediation** through our team of security experts.
- The MS-ISAC conducts **training sessions and webinars** across a broad array of cybersecurity related topics.
- We continually develop and distribute **strategic, tactical, and operational intelligence** to provide timely, actionable information to our members.
- We provide **cybersecurity resources** for the public, including daily tips, monthly newsletters, guides, and more.

Who We Serve

CISOs, CIOs, and other security professionals from:

- U.S. State, Local, Tribal, and Territorial governments
- U.S. State/Territory Homeland Security Advisors
- DHS-recognized Fusion Centers and local law enforcement entities

How We Do Business

- We cultivate a **collaborative environment** for information sharing.
- We focus on **readiness and response,** especially where the cyber and physical domains meet.
- We facilitate **partnerships** between the public and private sectors.
- We focus on **excellence** to develop industry-leading, cost-effective cybersecurity resources.
- **Collectively** we achieve much more than we can individually.

> **"All services performed by the MS-ISAC were not only prompt, but professional and efficient. Communication was handled very well and the report was fantastic."**
>
> **MS-ISAC Member**

Member Responsibilities

In order to maintain the MS-ISAC's trusted, collaborative environment, each member understands that the following principles of conduct will guide their actions.

Each member agrees to:

- Share appropriate information between and among the members to the greatest extent possible
- Recognize the sensitivity and confidentiality of the information shared and received
- Take all necessary steps to protect confidential information
- Transmit sensitive data to other members only through the use of agreed-upon secure methods
- Take all appropriate steps to help protect our critical infrastructure

Members are also asked to share their public-facing IP ranges and domain space with the MS-ISAC to facilitate efficient and effective discovery and notification of system compromises and potential vulnerabilities.

> "I will continue to leverage this expert and valuable service as long as it exists. The MS-ISAC CIRT was once again very efficient and provided a robust root cause analysis in a timely fashion."
>
> **MS-ISAC Member**

Reporting an Incident and Requesting Assistance

Members are encouraged to report incidents, even if they are not requesting assistance, to improve situational awareness for the benefit of all members.

Types of incidents to report include the following:

- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- Compromised password(s)
- Execution of malware, such as viruses, trojans, worms, ransomware, or botnet activity
- Defacement of a government web page
- Disruption or attempted denial of service (DoS)
- Unauthorized access to information
- Unauthorized use of a system for transmitting, processing, or storing data
- Unauthorized use or elevation of system privileges

If the cybersecurity incident you are reporting requires direct assistance, the CIRT, a unit comprised of highly trained and experienced staff, is able to assist you at no cost. Our incident response experts can assist with the following:

- Emergency conference calls
- Log analysis
- Mitigation and response recommendations
- Reverse engineering
- Threat Intelligence

REPORTING CYBERSECURITY INCIDENTS

To report an incident, please contact the SOC for 24×7×365 assistance:

Phone: **1-866-787-4722**

Email: **soc@cisecurity.org**

Security Operations of the MS-ISAC

No-cost Services

Compromised System Notifications

Provided to members in the event of a potential compromise identified based on the MS-ISAC's unique awareness of the threat landscape.

Cyber Incident Response Team (CIRT)

CIRT provides SLTT governments with malware analysis, computer and network forensics, malicious code analysis/mitigation, and incident response. External vulnerability assessments are also available post a cyber incident. This service helps victims of cyber incidents to check if their remediation efforts have been effective.

Cyber Threat Intelligence (CTI)

The CTI team collects, analyzes, and delivers actionable intelligence to operators and decision-makers responsible for defending SLTT governments. CTI maintains a curated, real-time, bi-directional indicator sharing platform which makes indicators available in the industry standard STIX/TAXII format at no cost to SLTTs and which can be integrated into local security operations. This platform is unique among the industry as it is tailored specifically for SLTTs.

Cyber Vulnerability and Threat Research

Analysts monitor federal government, third party, and open sources to identify, analyze, and then distribute pertinent intelligence.

Digital Forensics and Incident Response (DFIR)

CIS offers DFIR services to both MS-ISAC and EI-ISAC members at no cost, providing host and network forensics, understanding the root cause of a compromise, investigating insider threat activity, analyzing malware, and providing recommendations for remediating a cyber-attack.

Malicious Domain Blocking and Reporting (MDBR)

MDBR is a highly effective, no-cost solution available to both MS-ISAC and EI-ISAC members that proactively blocks network requests from an organization to known harmful web domains, helping protect IT systems against cybersecurity threats such as malware, phishing, and ransomware. Organizations are provided with weekly reports summarizing the potentially malicious requests that were detected. MDBR can be implemented in minutes, on existing systems, without additional hardware or software. Learn more on page 4.

National Liaison Team

The National Liaison Team is assigned to CISA Central to represent MS-ISAC and SLTT interests. CISA Central is a 24×7×365 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

Security Operations Center

The MS-ISAC operates within the SOC, which is a 24×7×365 joint security operations and analytical unit monitors, analyzes, and responds to cyber incidents targeting SLTT government entities.

The SOC provides real-time network monitoring and notification, early cyber threat warnings and advisories, and vulnerability identification and mitigation.

Malicious Domain Blocking and Reporting (MDBR)

The Malicious Domain Blocking and Reporting (MDBR) service is available for U.S. State, Local, Tribal, and Territorial (SLTT) government members of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), in partnership with the Cybersecurity and Infrastructure Security Agency (CISA) and Akamai. This service provides an additional layer of cybersecurity protection that is proven, effective, and easy to deploy.

About MDBR

MDBR technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.

REGISTER FOR MDBR

To register for MDBR, please visit https://mdbr.cisecurity.org/

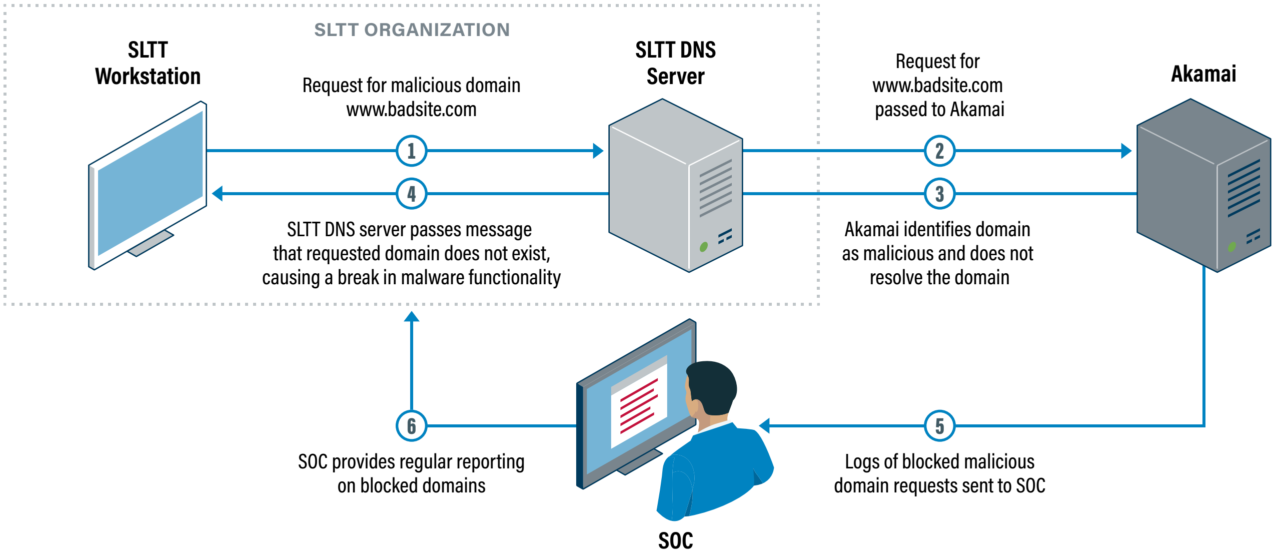
How MDBR Works

MDBR proactively blocks network traffic from an organization to known harmful web domains, helping protect IT systems against cybersecurity threats. Once an organization points its domain name system (DNS) requests to the Akamai's DNS server IP addresses, every DNS lookup will be compared against a list of known and suspected malicious domains. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, will be blocked and logged. CIS will then provide reporting that includes log information for all blocked requests and assist in remediation if needed.

The service is easy to implement and requires virtually no maintenance as CIS and Akamai fully maintain the systems required to provide the service.

Akamai provides all logged data to the SOC, including both successful and blocked DNS requests. This data will be utilized to perform detailed analysis and reporting for the betterment of the SLTT community and for organization-specific reporting for each SLTT organization that implements the service. CIS will provide regular reporting and intelligence services for SLTT members.

↓ Malicious Domain Blocking and Reporting Data Flow


SLTT ORGANIZATION
SLTT Workstation
Request for malicious domain www.badsite.com
1
SLTT DNS Server
4
SLTT DNS server passes message that requested domain does not exist, causing a break in malware functionality
Request for www.badsite.com passed to Akamai
2
Akamai
3
Akamai identifies domain as malicious and does not resolve the domain
6
SOC provides regular reporting on blocked domains
5
Logs of blocked malicious domain requests sent to SOC
SOC

Malicious Code Analysis Platform

The Malicious Code Analysis Platform (MCAP) is a web-based service that enables members to submit suspicious files, including executables, DLLs, documents, quarantine files, and archives for analysis in a controlled and non-public fashion. Additionally, the platform enables users to perform threat analysis based on domain, IP address, URL, hashes, and various Indicators Of Compromise (IOCs).

This platform allows users to obtain the results from analysis, behavioral characteristics, and additional detailed information that enables them to remediate the incident in a timely manner. This communication with our members provides the MS-ISAC with the situational awareness needed to assess the malware threat characteristics facing our SLTT government entities on a national level.

MCAP REGISTRATION

The Malicious Code Analysis Platform is available to all members free of charge. To register for an account, send an email to mcap@cisecurity.org using the following format:

Subject Line: **"MCAP Account Request"**

Body of the Email: **First and last name, name of government entity, email address.**

> "We so appreciate all that you have done to help! I can't tell you how much it helped to know that you were with us through this (incident)."
>
> **MS-ISAC Member**

Cyber Threat Intelligence and Analytical Products

Cyber Alert

Short and timely emails containing information on a specific cyber incident or threat.

Cybersecurity Advisories

Short and timely emails containing technical information regarding vulnerabilities in software and hardware.

Long-form Analytic Report (LFAR)

Lengthier, more in-depth threat intelligence reports with multiple assessments and confidence clearly articulated throughout.

Quarterly Threat Report (QTR)

Analyzes quarterly SLTT-focused cyber threat intelligence (CTI) trends and provides threat forecasting based on MS-ISAC internal and open-source reporting.

Short-form Analytic Report (SFAR)

Concise, easily digestible 1-2 page threat intelligence assessments with substantiation and analytic confidence clearly articulated.

Study

Strategic or operational view of a specific actor, group, campaign, malware family, nation state, or other collective target set of data. Studies take a longer view than other products, and while they may contain technical information, they are used primarily to support strategic conclusions, driving decision-making at higher levels, such as policy changes at the State and Federal level.

Weekly and Monthly IOCs

Reports highlighting malicious IPs and domains the MS-ISAC has identified through monitoring during the past week or month.

White Paper

Detailed technical papers providing key information about a topic of interest.

CIS SecureSuite Membership

CIS SecureSuite Membership provides integrated cybersecurity tools and resources to organizations of every size.

CIS SecureSuite Membership is FREE for U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

For more information or to register, please contact freesecuresuite@cisecurity.org.

Maintaining secure configurations are a complicated and time-consuming activity. Even if system configurations were secure to start with, the once-hardened IT environments will drift over time. You can effectively monitor your configurations, quickly identify vulnerabilities, and prevent configuration drift with CIS-CAT Pro. Your team can automate configuration assessments, conduct remote scans, implement security best practices, and more. CIS SecureSuite Membership is available at no cost to U.S. State, Local, Tribal, and Territorial (SLTT) government organizations.

CIS-CAT® Pro

CIS-CAT Pro combines the powerful security guidance of the CIS Controls and CIS Benchmarks into an assessment tool. Leveraging the CIS-CAT Pro Assessor and Dashboard components, users can view conformance to best practices and improve compliance scores over time.

- Select CIS Benchmarks annotated with CIS Controls mappings
- Semi-automated assessment of CIS Controls V7.1 Implementation Group 1 on Windows 10 and Windows Server with CIS Controls Assessment Module
- Multiple reporting formats (Microsoft Excel, HTML, etc.) with easy-to-view remediation steps for noncompliant settings
- Evidence-based reports which can be exported in various formats (HTML, XML, CSV, TXT)
- Remote assessment capability
- Vulnerability scanning functionality

CIS-CAT Pro Assessor works on-prem or in the cloud to scan target system configuration settings and reports compliance with corresponding CIS Benchmarks. Scans are typically completed in just a few minutes, saving users hours of tedious manual configuration review.

CIS-CAT Pro Dashboard consumes assessment reports and shows system compliance over time.

- CIS Controls view for annotated CIS Benchmark content
- View assessment results per-Benchmark or per-device
- Custom device tagging (PCI, admin, etc.) to view compliance for a group of systems
- Create exceptions to CIS Benchmark content and dynamically recalculate assessment scoring
- Alert notifications and difference reports for configuration drift between scans

CIS CSAT Pro

CIS CSAT Pro is an on-premises CIS Controls self-assessment tool that allows organizations to conduct, track, and assess their implementation of the CIS Controls.

- Collaborate across teams and assign user roles
- Choose which specific Sub-Controls to include
- Upload documentation as supporting evidence
- Track assessment over time
- Monitor alignment to other security frameworks
- Anonymously compare results to an industry average or other peer groups

CIS WorkBench

CIS WorkBench is a community platform where Members can collaborate and access resources.

https://workbench.cisecurity.org/

- Easily tailor CIS Benchmarks recommendations to fit organizational or compliance policies
- Export CIS Benchmarks in various formats (Microsoft Word, Microsoft Excel, XCCDF, OVAL, XML)
- CIS Build Kits (GPOs, Linux scripts, and more) for rapidly implementing CIS Benchmark recommendations

MS-ISAC Member Initiatives and Collaborative Resources

MS-ISAC membership enables entities to participate with their peers across the country, sharing knowledge, building relationships, and improving cybersecurity readiness and response.

Emergency Conference Calls

Members have access to conference calls to brief all members on major incidents or emerging events.

Monthly Member Threat Briefing

One-hour webcast briefings that provide members with updates on the threat landscape, status of national initiatives impacting them, and relevant news from members. DHS has a standing agenda item on each call.

Cyber Threat Briefings

The MS-ISAC provides cyber threat briefings to our members based on our expertise of the cyber threat landscape and incidents targeting SLTT governments.

Working Groups

Focused working committees to share ideas, generate recommendations, and produce deliverables to support the MS-ISAC and member-related programs (see page 8).

Members-Only Access to HSIN

The MS-ISAC has a Community of Interest (COI) on the Homeland Security Information Network (HSIN) which allows our membership a secure and confidential platform for sharing information. The COI includes the MS-ISAC cyber alert level map—a visual representation of the current cyber status of each state, updated on a monthly basis; and a library of policies, reports, guides, recorded webcasts, sector specific discussion groups, and many additional member resources.

REQUEST A SUBJECT MATTER EXPERT

MS-ISAC can provide subject matter experts for presentations and conferences.

Please reach out to info@cisecurity.org with your requests.

> **“It was very helpful to have the MS-ISAC to turn to at this difficult time. The MS-ISAC team was extremely helpful during every step of the project.”**
>
> **MS-ISAC Member**

MS-ISAC Working Groups

Working groups are voluntary committees focused on specific initiatives and deliverables in support of the MS-ISAC mission.

Who can participate in a working group?

Any member from any state, local, tribal, or territorial government.

What do the working groups do?

They serve a significant role in the creation and implementation of MS-ISAC initiatives. These working groups are also a tremendous opportunity to collaborate with your peers across the country. They identify current issues facing SLTT governments and help determine the future course of addressing cybersecurity challenges. They have been responsible for:

- Authoring the Nationwide Cybersecurity Review (NCSR) question set and analyzing the results
- Participating in the development and execution of cybersecurity tabletop exercises
- Increasing participation in Cybersecurity Awareness Month activities
- Authoring the monthly newsletter and other publications

How much time will I need to commit?

- Level of commitment varies by group
- Extent of involvement is completely your choice

Current Working Groups

Business Resiliency

Focuses on the processes, tools, and best practices related to public sector business continuity and recovery—not only of technology assets, but also recovery of the entire organization, including people, locations, and communications.

Cybersecurity Metrics

Focuses on recommending and implementing methodologies to help SLTT entities with cybersecurity metrics and compliance inventory, assessment, and audit of their cybersecurity assets. This group works jointly with DHS, National Association of State Chief Information Officers (NASCIO) and the National Association of Counties (NACo) to support the DHS Nationwide Cybersecurity Review.

K-12

Brings together a diverse group of educational agencies, in hopes of better understanding the issues, challenges and concerns of school districts throughout the country. The working group strives to meet those needs and improve the overall cybersecurity posture of the community to support the overall mission of the MS-ISAC.

Education and Awareness

Focuses on implementing innovative strategies, improving existing programs, and promoting successful localized initiatives for national cybersecurity education, awareness, and training content to support the overall mission of the MS-ISAC.

Leadership Mentoring Program

Designed to build meaningful and mutually beneficial relationships between cybersecurity professionals to promote increased maturity of leaders and programs across the SLTT community.

SHARE YOUR EXPERTISE BY JOINING A WORKING GROUP TODAY!

Send an email to info@cisecurity.org with "Working Group Request" in the subject line, and include the following:

- **Name**
- **Working Group of interest**
- **Entity/Agency name**
- **Email and telephone number**

> "I can honestly say that your organization has made an immediate impact in our overall security readiness. Thank you."

MS-ISAC Member

Nationwide Cybersecurity Review

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment designed to evaluate cybersecurity maturity. The Senate Appropriations Committee has requested an ongoing effort to chart nationwide progress in cybersecurity and identify emerging areas of concern. In response, DHS has partnered with the MS-ISAC, NASCIO, and NACo to develop and conduct the NCSR.

Who can participate?

All states (and agencies), local governments (and departments), and tribal and territorial governments.

How does the NCSR work?

- Hosted on a secure portal
- Based on the NIST Cybersecurity Framework
- Based on key milestone activities for information risk management
- Closely aligned with security governance processes and maturity indexes embodied in accepted standards and best practices
- Covers the core components of cybersecurity and privacy programs

When does the survey take place?

The survey will be available from October through February. For more information and to register, visit cisecurity.org/ms-isac/services/ncsr/.

Advantages of participation

- Access to NIST, COBIT, ISO and CIS Controls informative references
- Free and voluntary self-assessment to evaluate your cybersecurity posture
- Customized reports to help you understand your cybersecurity maturity, including:
  - A detailed report of your responses along with recommendations to improve your organization's cybersecurity posture
  - Additional summary reports that gauge your cybersecurity measures against peers (using anonymized data)
  - Insight to help prioritize your effort to develop security controls
- Benchmarks to gauge your own year-to-year progress
- Metrics to assist in cybersecurity investment justifications
- Contribute to the nation's cyber risk assessment process

The Survey

The NCSR provides survey participants with instructions and guidance. Additional support is available, including supplemental documentation at the link listed below and the ability to contact the NCSR help desk.

Once the NSCR is complete, participants will have immediate access to an individualized report measuring the level of adoption of security controls within their organization. This report includes recommendations on how to raise your organization's risk awareness.

The MS-ISAC and DHS will review all aggregate data and share a high-level summary with all participants. The names of participants and their organizations will not be identified in this report. This report is provided to Congress in alternate years to highlight cybersecurity gaps and capabilities among our state, local, territorial and tribal governments.

DID YOU KNOW?

State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) grant recipients are now required to complete the NCSR. These grants include funds that can be used to enhance the cybersecurity maturity of organizations. Learn more at www.fema.gov/grants/preparedness/homeland-security.

Cybersecurity Education

The MS-ISAC produces numerous communications to engage our members and help national efforts for better cybersecurity.

Education and Awareness Materials

Monthly Newsletters: These newsletters use non-technical language, and they can be rebranded to suit individual member needs. Newsletter topics include details on the most current threats and suggested best cybersecurity practices.

Monthly Webinars: These feature timely topics and experts from the public and private sector sharing insight on addressing cyber challenges and are open to the public.

Cybersecurity Awareness Toolkit

The Cybersecurity Awareness Toolkit features educational materials designed to raise cybersecurity awareness. Digital materials are aggregated for your use.

FedVTE

The Federal Virtual Training Environment (FedVTE) is DHS' online, on-demand training center. FedVTE provides SLTT IT professionals with hands-on labs and training courses. https://fedvte.usalearning.gov/

Best of the Web Contest

The MS-ISAC conducts an annual Best of the Web contest to recognize SLTTs to be inclusive of tribes, education, etc., who use their websites to promote cybersecurity. We review the cybersecurity websites for all 50 state governments and the many local governments that decide to participate. The judging is based upon several criteria including cybersecurity content, usability, accessibility, and appearance.

The contest recognizes outstanding websites and highlights them as examples for others to consider when they are developing or redesigning their own sites.

The Best of the Web contest kicks off in the beginning of October, which is Cybersecurity Awareness Month. The winners are announced on the November ISAC Monthly Membership Call.

Poster Contest

The MS-ISAC conducts an annual Kids Safe Online poster contest to encourage young people to create cybersecurity messages that any end-user can apply to their own life.

The contest is open to all public, private, or home-schooled students in kindergarten through twelfth grade. Winning entries of the MS-ISAC Kids Safe Online poster contest are what make up the next year's MS-ISAC Cybersecurity Awareness Toolkit, which is shared digitally with MS-ISAC members.

The MS-ISAC Kids Safe Online poster contest is launched at the beginning of Cybersecurity Awareness Month, and submissions are due the following January.

FOR MORE INFORMATION

For questions regarding education and awareness materials or participation in any of these programs, please contact info@cisecurity.org.

For more information on DHS services, visit www.cisa.gov.

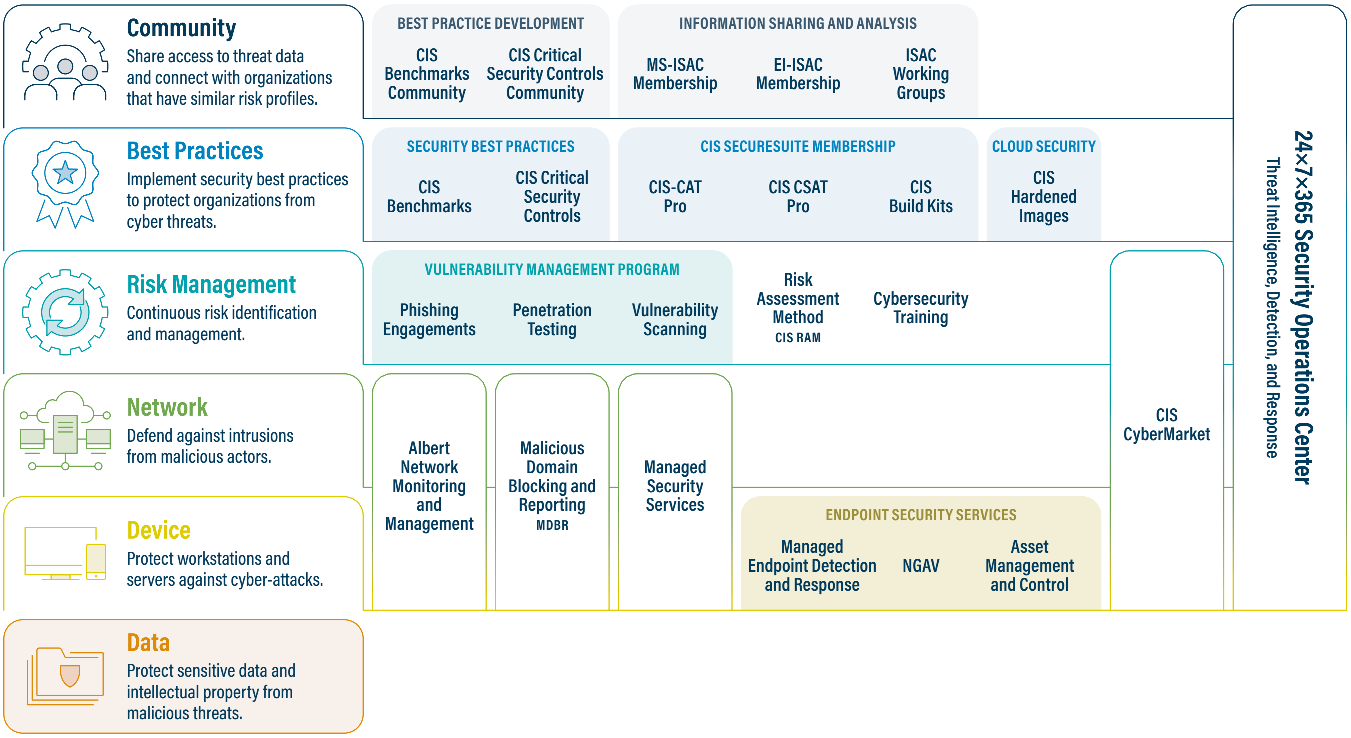
Item 9.

Fee-based Services

As the complexity of cyber-attacks continue to evolve and the frequency of those cyber-attacks increase, organizations must apply a defense-in-depth approach to ensure their ability to protect, prevent, detect, respond to, and recover from external and internal attacks. Since there is no single technology or set of controls that will provide a complete solution, this layered, risk-based approach to security is essential, regardless of the size, complexity, or vertical industry of the organization.

CIS has architected security solutions with the critical nature of defense-in-depth in mind. U.S. SLTT government organizations can deploy a defense-in-depth strategy to significantly improve their cybersecurity posture with these services offered by CIS, the MS-ISAC, and the EI-ISAC.

The CIS Defense-in-depth Model ↓



Community
Share access to threat data and connect with organizations that have similar risk profiles.

BEST PRACTICE DEVELOPMENT
CIS Benchmarks Community
CIS Critical Security Controls Community

INFORMATION SHARING AND ANALYSIS
MS-ISAC Membership
EI-ISAC Membership
ISAC Working Groups

Best Practices
Implement security best practices to protect organizations from cyber threats.

SECURITY BEST PRACTICES
CIS Benchmarks
CIS Critical Security Controls

CIS SECURESUITE MEMBERSHIP
CIS-CAT Pro
CIS CSAT Pro
CIS Build Kits

CLOUD SECURITY
CIS Hardened Images

Risk Management
Continuous risk identification and management.

VULNERABILITY MANAGEMENT PROGRAM
Phishing Engagements
Penetration Testing
Vulnerability Scanning

Risk Assessment Method
CIS RAM

Cybersecurity Training

Network
Defend against intrusions from malicious actors.

Device
Protect workstations and servers against cyber-attacks.

Albert Network Monitoring and Management

Malicious Domain Blocking and Reporting
MDBR

Managed Security Services

ENDPOINT SECURITY SERVICES
Managed Endpoint Detection and Response
NGAV
Asset Management and Control

CIS CyberMarket

24×7×365 Security Operations Center
Threat Intelligence, Detection, and Response

Data
Protect sensitive data and intellectual property from malicious threats.

Vulnerability and Risk Management

CIS provides cost-effective vulnerability management solutions for networks and web applications as well as penetration testing. Some services include:

- Network discovery and mapping
- Vulnerability assessment reporting
- Testing vulnerabilities for false-positives
- Identification of high-value assets
- Prioritizing vulnerabilities based on risk

Our network and web application penetration testing services simulate a real-world cyber-attack. Taking the vantage point of an attacker, our experts attempt to exploit vulnerabilities in an organization's IT infrastructure in order to determine the likelihood and potential scope of a cyber-attack. At the conclusion of testing, the findings are delivered in a detailed report, with prioritized remediation recommendations.

CIS Endpoint Security Services (ESS)

CIS ESS offers device-level protection and response to strengthen an organization's cybersecurity program, and provides active defense against both known (signature-based) and unknown (behavioral-based) malicious activity, as well as effective defense against encrypted malicious traffic. The service includes various measures to protect endpoint devices and is fully monitored and managed 24×7×365 by our SOC. CIS ESS can stop an attack in its tracks upon identifying a threat on an endpoint, regardless of the network it is connected to, taking an active role in mitigating and remediating malware affecting an organization's devices by killing or quarantining files.

Managed Security Services

The 24×7×365 SOC provides SLTT entities cost-effective log and security event monitoring of existing devices including, but not limited to, IDS/IPS, firewalls, switches and routers, servers, endpoints, and web proxies. Actionable items are escalated to organizations as an alert and our 24×7×365 SOC is always on hand to answer questions regarding alerts or notifications received.

CIS CyberMarket®

The CIS CyberMarket assists SLTT governments and nonprofit entities in achieving a greater cybersecurity posture through trusted expert guidance and cost-effective procurement. The CIS CyberMarket builds public and private partnerships and works to enhance collaboration that improves the nation's cybersecurity posture. The CIS CyberMarket makes cybersecurity purchasing effective, easy, and economical. Discounts include:

- Training
- Software
- Consulting Services

FOR MORE INFORMATION

If you would like more information about these services or a quote, please contact CIS at services@cisecurity.org.

> **"The assistance from the MS-ISAC during a very stressful time has been much appreciated. It's comforting to know that we have your skills, knowledge, and expertise ready to assist."**

MS-ISAC Member

Albert Network Monitoring and Management

Albert is a cost-effective Intrusion Detection System (IDS) available to SLTT entities, including election organizations, critical infrastructure, and public education. This service is committed to building and maintaining the most comprehensive set of detection rules and signatures in order to quickly and accurately identify threats impacting SLTT entities.

Turnkey solution incorporating 24×7×365 monitoring and management.

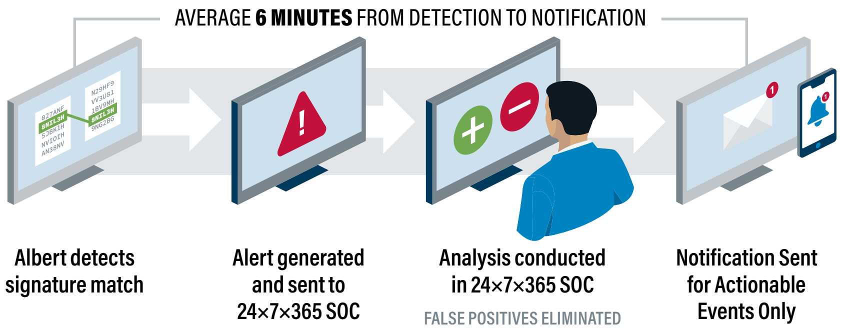
Utilizes commercial, open-source, and custom signatures developed from leveraging our federal partners for access to recently de-classified signatures, indicators CIS derives from incident response cases, as well as member submitted and third-party threat data.

> **"Within 2 seconds of the script being launched, the computer was automatically isolated from the network. I had set a rule so any critical items like this would cause the PC to be isolated. We received the initial MS-ISAC email at 11:29, 1 minute after script launch. I would say our protection systems worked as well as we could hope."**
>
> **City Member**

Why is the Albert Service Unique?

- Government-specific focus and tailored to SLTT governments' cybersecurity needs.
- Experienced cybersecurity analysts review each cybersecurity event, which results in minimizing the number of false-positive notifications. This system allows first responders to focus on actionable events.
- Correlation of data from multiple public and private partners:
  - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties.
  - When a major new threat is identified, the MS-ISAC will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats. If abnormal traffic patterns are detected, analysts review the traffic to determine the cause, looking for malicious traffic that is not detected by signatures.
- Signatures from forensic analysis of hundreds of SLTT governments cyber incidents are added to the signature repository.
- Integration of research on threats specific to SLTT governments, including nation-state attacks.
- MS-ISAC staff are deployed at the CISA Central in Arlington, VA. This liaison relationship facilitates valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Availability of a CIRT for forensic and malware analysis which is part of the no-cost MS-ISAC membership.
- Cost-effective solution that is significantly less expensive than the purchase and maintenance of a typical commercial IDS solution.

↓ Albert notification cycle


AVERAGE **6 MINUTES** FROM DETECTION TO NOTIFICATION
Albert detects signature match
Alert generated and sent to 24×7×365 SOC
Analysis conducted in 24×7×365 SOC
FALSE POSITIVES ELIMINATED
Notification Sent for Actionable Events Only

CIS Center for Internet Security®

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
☎ 518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity

Item 9.

CYBER ASSESSMENT FACT SHEET

Vulnerability Scanning

September 2023

OVERVIEW

CISA's Vulnerability Scanning (VS) is persistent "internet scanning-as-a-service" and part of CISA's service offerings. VS service continuously assesses the health of your internet-accessible assets by checking for known vulnerabilities, weak configurations—or configuration errors—and suboptimal security practices. VS service also recommends ways to enhance security through modern web and email standards.

VS service includes:

- **Target Discovery** identifies all active internet-accessible assets (networks, systems, and hosts) to be scanned
- **Vulnerability Scanning** initiates non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

OBJECTIVES

- Maintain enterprise awareness of your internet-accessible systems.
- Provide insight into how systems and infrastructure appear to potential attackers.
- Drive proactive mitigation of vulnerabilities and reduce risk

PHASES

Pre-Planning	Planning	Execution	Post-Execution
Stakeholder: • Requests service. • Provides target list (scope) • Signs and returns documents	**CISA:** • Confirms scanning schedule • Sends pre-scan notification to stakeholder	**CISA:** • Performs initial scan of submitted scope • Rescans scope based on detected vulnerability severity: ⇒ 12 hours for "critical" ⇒ 24 hours for "high" ⇒ 4 days for "medium" ⇒ 6 days for "low" ⇒ 7 days for "no vulnerabilities"	**CISA:** • Delivers weekly report to stakeholder • Provides vulnerability mitigation recommendations to stakeholder • Provides detailed findings in consumable format to stakeholder

HOW TO GET STARTED

Contact vulnerability@cisa.dhs.gov to get started. Please keep in mind:

- CISA's assessments are available to both public and private organizations at no cost.
- Service availability is limited; service delivery timelines are available upon request. CISA prioritizes service delivery queues on a continuous basis to ensure no stakeholder/sector receives a disproportionate allocation of resources and the data collected is a diverse representation of the nation.

Item 9.

CIS Center for Internet Security®

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

NIST Cybersecurity Framework

Policy Template Guide

CIS Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

Contents

CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Introduction

The Multi-State Information Sharing & Analysis Center (MS-ISAC) is offering this guide to participants of the Nationwide Cybersecurity Review (NCSR) and MS-ISAC members, as a resource to assist with the application and advancement of cybersecurity policies.

The policy templates are provided courtesy of the SANS Institute (https://www.sans.org/), the State of New York, and the State of California. The templates can be customized and used as an outline of an organizational policy, with additional details to be added by the end user.

The NCSR question set represents the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This guide gives the correlation between 49 of the NIST CSF subcategories, and applicable policy and standard templates. A NIST subcategory is represented by text, such as "ID.AM-5." This represents the NIST function of Identify and the category of Asset Management.

For additional information on services provided by the Multi-State Information Sharing & Analysis Center (MS-ISAC), please refer to the following page: https://www.cisecurity.org/ms-isac/services/. These policy templates are also mapped to the resources MS-ISAC and CIS provide, open source resources, and free FedVTE training: https://www.cisecurity.org/wp-content/uploads/2019/11/Cybersecurity-Resources-Guide.pdf.

Disclaimer: These policies may not reference the most recent applicable NIST revision, however may be used as a baseline template for end users.

NIST FUNCTION:

Identify

Identify: Asset Management (ID.AM)

ID.AM-1 **Physical devices and systems within the organization are inventoried.**

↗Acceptable Use of Information Technology Resource Policy
Access Control Policy
Account Management/Access Control Standard
Identification and Authentication Policy
Information Security Policy
Security Assessment and Authorization Policy
Security Awareness and Training Policy

ID.AM-2 **Software platforms and applications within the organization are inventoried.**

Acceptable Use of Information Technology Resource Policy
Access Control Policy
Account Management/Access Control Standard
Identification and Authentication Policy
Information Security Policy
Security Assessment and Authorization Policy
Security Awareness and Training Policy

ID.AM-4 **External information systems are catalogued.**

System and Communications Protection Policy

ID.AM-5 **Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value).**

SANS Policy Template: Acquisition Assessment Policy
Information Classification Standard
Information Security Policy

ID.AM-6 **Cybersecurity roles and responsibilities for the entire workforces and third-party stakeholders (e.g. suppliers, customers, partners) are established.**

Acceptable Use of Information Technology Resource Policy
Information Security Policy
Security Awareness and Training Policy

Identify: Risk Management Strategy (ID.RM)

ID.RM-1 **Risk management processes are established, managed, and agreed to by organizational stakeholders.**

Information Security Policy
Information Security Risk Management Standard
Risk Assessment Policy

Identify: Supply Chain Risk Management (ID.SC)

ID.SC-2 **Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.**

SANS Policy Template: Acquisition Assessment Policy
Identification and Authentication Policy
Security Assessment and Authorization Policy
Systems and Services Acquisition Policy

ID.SC-4 **Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.**

SANS Policy Template: Acquisition Assessment Policy
Identification and Authentication Policy
Security Assessment and Authorization Policy
Systems and Services Acquisition Policy

ID.SC-5 **Response and recovery planning and testing are conducted with suppliers and third-party providers.**

SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Systems and Services Acquisition Policy

NIST FUNCTION

Protect

Protect: Identity Management and Access Control (PR.AC)

PR.AC-1 **Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.**

Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

PR.AC-3 **Remote access is managed.**

SANS Policy Template: Remote Access Policy
Remote Access Standard

PR.AC-4 **Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.**

Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

PR.AC-5 **Network integrity is protected (e.g., network segregation, network segmentation).**

SANS Policy Template: Lab Security Policy
SANS Policy Template: Router and Switch Security Policy
802.11 Wireless Network Security Standard
Mobile Device Security
System and Information Integrity Policy

Protect: Awareness and Training (PR.AT)

PR.AT-1 **All users are informed and trained.**

Acceptable Use of Information Technology Resources Policy
Information Security Policy
Personnel Security Policy
Physical and Environmental Protection Policy
Security Awareness and Training Policy

Protect: Data Security (PR.DS)

PR.DS-1 **Data-at-rest is protected**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Encryption Standard
Incident Response Policy
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard

PR.DS-2 **Data-in-transit is protected.**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Encryption Standard
Incident Response Policy
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard

PR.DS-3 **Assets are formally managed throughout removal, transfers, and disposition.**

SANS Policy Template: Acquisition Assessment Policy
SANS Policy Template: Technology Equipment Disposal Policy
Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

PR.DS-7 **The development and testing environment(s) are separate from the production environment.**

SANS Policy Template: Lab Security Policy
SANS Policy Template: Router and Switch Security Policy

PR.DS-8 **Integrity checking mechanisms are used to verify hardware integrity.**

SANS Policy Template: Acquisition Assessment Policy
System and Information Integrity Policy

Protect: Information Protection Processes and Procedures (PR.IP)

PR.IP-1 **A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality).**

Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard

PR.IP-4 **Backups of information are conducted, maintained, and tested.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Encryption Standard
Incident Response Policy
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard

PR.IP-6 **Data is destroyed according to policy.**

SANS Policy Template: Technology Equipment Disposal Policy
Maintenance Policy
Media Protection Policy
Sanitization Secure Disposal Standard

PR.IP-9 **Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Disaster Recovery Plan Policy
SANS Policy Template: Pandemic Response Planning
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Planning Policy

PR.IP-10 **Response and recovery plans are tested.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Disaster Recovery Plan Policy
SANS Policy Template: Pandemic Response Planning
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Planning Policy

Protect: Maintenance (PR.MA)

PR.MA-2 **Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.**

SANS Policy Template: Remote Access Policy
SANS Policy Template: Remote Access Tools Policy
Maintenance Policy
Remote Access Standard
Security Logging Standard

Protect: Protective Technology (PR.PT)

PR.PT-1 **Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.**

SANS Policy Template: Information Logging Standard
Access Control Policy
Account Management/Access Control Standard
Authentication Tokens Standard
Configuration Management Policy
Identification and Authentication Policy
Sanitization Secure Disposal Standard
Secure Configuration Standard
Secure System Development Life Cycle Standard
Security Logging Standard

PR.PT-2 **Removable media is protected and its use restricted according to policy.**

SANS Policy Template: Acceptable Use Policy
Acceptable Use of Technology Resources Policy
Media Protection Policy
Mobile Device Security

PR.PT-4 **Communications and control networks are protected.**

SANS Policy Template: Router and Switch Security Policy
Encryption Standard
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
System and Communications Protection Policy

PR.PT-5 **Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.**

SANS Policy Template: Disaster Recovery Plan Policy
SANS Policy Template: Security Response Plan Policy

NIST FUNCTION:

Detect

Detect: Anomalies and Events (DE.AE)

DE.AE-3 **Event data are collected and correlated from multiple sources and sensors.**

SANS Policy Template: Information Logging Standard
Auditing and Accountability Standard
Security Logging Standard
System and Information Integrity Policy
Vulnerability Scanning Standard

Detect: Security Continuous Monitoring (DE.CM)

DE.CM-1 **The network is monitored to detect potential cybersecurity events.**

SANS Policy Template: Router and Switch Security Policy
Encryption Standard
Information Security Policy
Maintenance Policy
Media Protection Policy
Mobile Device Security
Patch Management Standard
Security Assessment and Authorization Policy
Vulnerability Scanning Standard

DE.CM-4 **Malicious code is detected.**

Auditing and Accountability Standard
Secure Coding Standard
Security Logging Standard
System and Information Integrity Policy
Vulnerability Scanning Standard

DE.CM-7 **Monitoring for unauthorized personnel, connections, devices, and software is performed.**

Auditing and Accountability Standard
Security Logging Standard
System and Information Integrity Policy
Vulnerability Scanning Standard

Detect: Detection Processes (DE.DP)

DE.DP-1 **Roles and responsibilities for detection are well defined to ensure accountability.**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Information Security Policy

DE.DP-4 **Event detection information is communicated.**

Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Information Security Policy

NIST FUNCTION:

Respond

Respond: Response Planning (RS.RP)6

RS.RP-1 **Response plan is executed during or after an event.**

SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy
Planning Policy

Respond: Communications (RS.CO)

RS.CO-1 **Personnel know their roles and order of operations when a response is needed.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RS.CO-2 **Incidents are reported consistent with established criteria.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RS.CO-3 **Information is shared consistent with response plans.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RS.CO-4 **Coordination with stakeholders occurs consistent with response plans**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RS.CO-5 **Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

Respond: Analysis (RS.AN)

RS.AN-4 **Incidents are categorized consistent with response plans.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

Respond: Improvements (RS.IM)

RS.IM-1 **Response plans incorporate lessons learned.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RS.IM-2 **Response strategies are updated.**

SANS Policy Template: Data Breach Response Policy
SANS Policy Template: Pandemic Response Planning Policy
SANS Policy Template: Security Response Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

NIST FUNCTION:

Recover

Recover: Recovery Planning (RC.RP)

RC.RP-1 **Recovery plan is executed during or after a cybersecurity incident.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Contingency Planning Policy
Cyber Incident Response Standard
Incident Response Policy

Recover: Improvements (RC.IM)

RC.IM-1 **Recovery plans incorporate lessons learned.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Contingency Planning Policy
Cyber Incident Response Standard
Incident Response Policy

RC.IM-2 **Recovery strategies are updated.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Contingency Planning Policy
Cyber Incident Response Standard
Incident Response Policy

Recover: Communications (RC.CO)

RC.CO-1 **Public relations are managed.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RC.CO-2 **Reputation is repaired after an incident.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

RC.CO-3 **Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.**

SANS Policy Template: Disaster Recovery Plan Policy
Computer Security Threat Response Policy
Cyber Incident Response Standard
Incident Response Policy

Item 9.

CIS® Center for Internet Security®

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Additional Policy Templates

The following policy templates address additional functions and processes related to an organization's information security:

General

Acceptable Encryption Policy
Clean Desk Policy
Digital Signature Acceptance Policy
Email Policy
Ethics Policy
Password Construction Guidelines
Password Protection Policy
Secure Use of Social Media Guideline
Continuing Professional Education Requirements for Information Security Officers/ Designated Security Representatives
Information Security Exception Policy

Network

Bluetooth Baseline Requirements Policy
Wireless Communication Policy
Wireless Communication Standard

Server Security

Database Credentials Policy Server Security Policy
Software Installation Policy
Workstation Security (For HIPAA) Policy

Application Security

Web Application Security Policy

IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Item 9.

DEFEND TODAY,
SECURE TOMORROW

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE EXTERNAL DEPENDENCIES MANAGEMENT (EDM) ASSESSMENT ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGAIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTERED BY REGIONALLY-LOCATED CYBERSECURITY ADVISORS, THE ASSESSMENT PROVIDES AN ORGANIZATION WITH A BETTER UNDERSTANDING OF HOW THEY MANAGE RISKS ARISING FROM DEPENDENCES ON THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN.

FORMAT AND GOALS

The EDM Assessment is conducted as a four-hour session at a location of your choosing and facilitated by trained DHS representatives. Your organization can use the assessment by itself and as the first step in an improvement effort. You also may use it in conjunction with CISA's External Dependencies Management Method, which provides a rigorous, repeatable way to identify and manage specific suppliers or other external entities that your organization depends on to support its mission.

The goals of the assessment are to:

- Evaluate the activities and practices your organization uses to manage risks arising from external dependencies.
- Provide an objective review of your organization's capabilities in the assessed areas and recommendations offering a roadmap for improvement based on industry-leading practices.

APPROACH

Risks associated with the ICT supply chain have grown dramatically with expanded outsourcing of technology and infrastructure. Failures in managing these risks have resulted in incidents affecting millions of people.

The EDM Assessment focuses on the relationship between your organization's high-value services and assets (people, technology, facilities, and information) and evaluates how you manage risks incurred from using the ICT supply chain to support these high-value services. The ICT supply chain consists of outside parties that operate, provide, or support information and communications technology. Common examples include externally provided web and data hosting, telecommunications services, and data centers, as well as any service that depends on the secure use of ICT.

Through the EDM Assessment, your organization will evaluate:

- Relationship Formation – how your organization considers third-party risks, selects external entities, and forms relationships with them so that risk is managed from the start.
- Relationship Management and Governance – how your organization manages ongoing relationships with external entities to support and strengthen your critical services at a managed level of risk and costs.

- Service Protection and Sustainment – how your organization plans for, anticipates, and manages disruption or incidents related to external entities.

The EDM Assessment evolved from the DHS Cyber Resilience Review (CRR) and, like the CRR, is based on the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute.

BENEFITS AND OUTCOMES

Through an EDM Assessment, your organization will gain a better understanding of your cybersecurity posture relating to external dependencies. The assessment provides:

- An opportunity for participants from different parts of you organization to discuss issues relating to vendors and reliance on external entities;
- Options for consideration that guide improvement efforts, using recognized standards and best practices drawn from such sources as the CERT-RMM, NIST standards, and the NIST Cybersecurity Framework; and
- A comprehensive report on your third-party risk management practices and capabilities.

DATA PRIVACY

The EDM Assessment report is created exclusively for your organization's internal use. All data collected and analysis performed during an EDM assessment is afforded protection under the CISA Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that CISA employees are trained in the safeguarding and handling of PCII, CISA cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

PARTICIPANTS

To conduct an EDM assessment, CISA recommends that you involve a cross-functional team that includes those responsible for the functions shown in the following.

- IT security planning and management (e.g., Director of Information Technology)
- IT operations (e.g., configuration/change managers)
- Risk managers, in particular operations risk (e.g., enterprise/operations risk manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- IT policy and governance (e.g., Chief Information Security Officer)
- Business management (e.g., operations manager)
- Procurement and vendor management (e.g., contracts and legal support managers)
- Legal

For further information, contact your Cybersecurity Advisor (CSA) at iodregionaloperations@cisa.dhs.gov.

Item 9.

Hospital Vendor Contract Summary Sheet

1. ☐ **Existing Vendor** ☒ **New Vendor**

2. **Name of Contract: Cybersecurity & Infrastructure Security Agency**

3. **Contract Parties:**

4. **Contract Type Services:**

5. **Impacted Hospital Departments:** Hospital Infrastructure

Summary: To enhance our hospital's cybersecurity posture, the following no-cost services and resources are offered by CISA:

1. Vulnerability Scanning
2. Hospital-Specific Resources
3. Workshops
4. Cybersecurity Evaluation Tool (CSET)
5. Tabletop Exercises (TTX)
6. Training Opportunities
7. Cybersecurity Grant Program
8. MS-ISAC Services

By implementing these measures, we can strengthen our hospital’s defenses against cyber threats and ensure compliance with national cybersecurity standards.

6. **Cost:** None

7. **Term:**

8. **Termination Clause:**

9. **Other:**

IT Security

Supply Chain

OT Security

Insider Threat

Physical Security

Interoperable Communications

Item 9.

DEFEND TODAY,
SECURE TOMORROW

CYBER RESILIENCE REVIEW

THE PRESIDENTIAL POLICY DIRECTIVE (PPD) 41, UNITED STATES CYBER INCIDENT COORDINATION, SETS FORTH THE PRINCIPLES GOVERNING THE FEDERAL GOVERNMENT'S RESPONSE TO CYBER INCIDENTS AND ESTABLISHES LEAD AGENCIES AND PLANS FOR COORDINATING THE BROADER FEDERAL GOVERNMENT RESPONSE FOR THE AFFECTED ENTITIES, OR VICTIMS, OF SUCH INCIDENTS.

FORMAT AND GOAL

CISA offers two options for the CRR: a downloadable self-assessment and a facilitated six-hour session with trained DHS representatives at your locations.

Through the CRR, the organization will develop an understanding of its operational resilience and ability to manage cyber risk during normal operations and times of operational stress and crisis.

APPROACH

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring and defining cybersecurity capabilities across 10 domains:

- Asset Management,
- Controls Management,
- Configuration and Change Management,
- Vulnerability Management,
- Incident Management,
- Service Continuity Management,
- Risk Management,
- External Dependencies Management,
- Training and Awareness, and
- Situational Awareness.

PARTICIPANTS

To conduct a CRR, CISA recommends that you involve a cross-functional team representing business, operations, security, information technology, and maintenance areas, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)

Item 9.

- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)

BENEFITS AND OUTCOMES

The CRR provides a better understanding of an organization's cybersecurity posture. The review provides an improved organization-wide awareness of the need for effective cybersecurity management; a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis; a verification of management success; a catalyst for dialog between participants from different functional areas within your organization; and a comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards and best practices as well as references to the CERTRMM.

DATA PRIVACY

The CRR report is created exclusively for your organization's internal use. All data collected and analysis performed during a CRR assessment is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

ASSOCIATION TO THE CYBERSECURITY FRAMEWORK

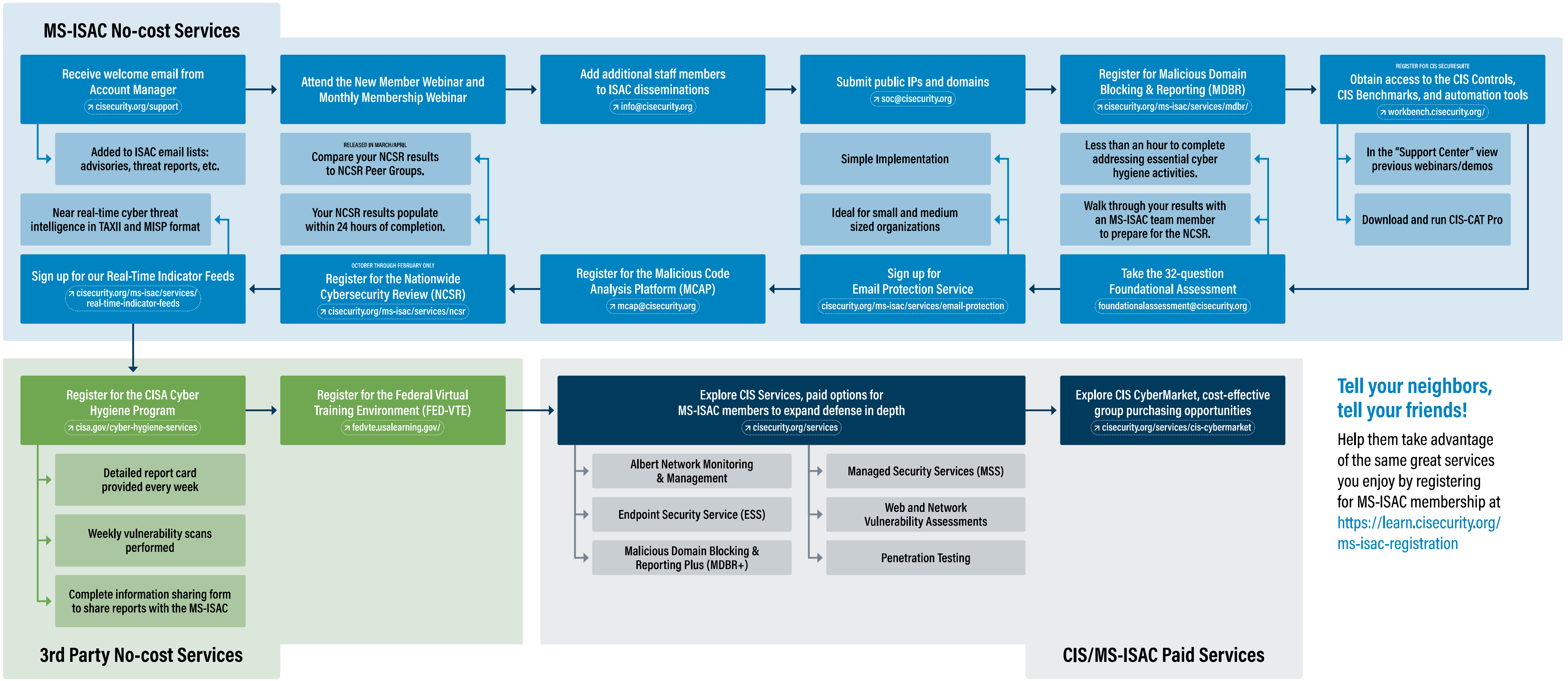
The principles and recommended practices within the CRR align with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps and, where appropriate, recommended improvement efforts. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.

For further information, contact your Cybersecurity Advisor (CSA) at
CISA.IOD.Region.R01_cyber_security@cisa.dhs.gov

Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

MS-ISAC Enrollment Guide



MS-ISAC No-cost Services

Receive welcome email from Account Manager ↗ cisecurity.org/support

Added to ISAC email lists: advisories, threat reports, etc.

Attend the New Member Webinar and Monthly Membership Webinar

Add additional staff members to ISAC disseminations ↗ info@cisecurity.org

Submit public IPs and domains ↗ soc@cisecurity.org

Simple Implementation

Ideal for small and medium sized organizations

Register for Malicious Domain Blocking & Reporting (MDBR) ↗ cisecurity.org/ms-isac/services/mdbr/

Less than an hour to complete addressing essential cyber hygiene activities.

Walk through your results with an MS-ISAC team member to prepare for the NCSR.

REGISTER FOR CIS SECURESUITE

Obtain access to the CIS Controls, CIS Benchmarks, and automation tools ↗ workbench.cisecurity.org/

In the "Support Center" view previous webinars/demos

Download and run CIS-CAT Pro

Take the 32-question Foundational Assessment foundationalassessment@cisecurity.org

Sign up for Email Protection Service cisecurity.org/ms-isac/services/email-protection

Register for the Malicious Code Analysis Platform (MCAP) ↗ mcap@cisecurity.org

OCTOBER THROUGH FEBRUARY ONLY

Register for the Nationwide Cybersecurity Review (NCSR) ↗ cisecurity.org/ms-isac/services/ncsr

RELEASED IN MARCH/APRIL

Compare your NCSR results to NCSR Peer Groups.

Your NCSR results populate within 24 hours of completion.

Sign up for our Real-Time Indicator Feeds ↗ cisecurity.org/ms-isac/services/real-time-indicator-feeds

Near real-time cyber threat intelligence in TAXII and MISP format

3rd Party No-cost Services

Register for the CISA Cyber Hygiene Program ↗ cisa.gov/cyber-hygiene-services

Detailed report card provided every week

Weekly vulnerability scans performed

Complete information sharing form to share reports with the MS-ISAC

Register for the Federal Virtual Training Environment (FED-VTE) ↗ fedvte.usalearning.gov/

CIS/MS-ISAC Paid Services

Explore CIS Services, paid options for MS-ISAC members to expand defense in depth ↗ cisecurity.org/services

Albert Network Monitoring & Management

Endpoint Security Service (ESS)

Malicious Domain Blocking & Reporting Plus (MDBR+)

Managed Security Services (MSS)

Web and Network Vulnerability Assessments

Penetration Testing

Explore CIS CyberMarket, cost-effective group purchasing opportunities ↗ cisecurity.org/services/cis-cybermarket

Tell your neighbors, tell your friends!

Help them take advantage of the same great services you enjoy by registering for MS-ISAC membership at https://learn.cisecurity.org/ms-isac-registration

Item 10.

eClinicalWorks

WORK ORDER

Client Name:	Mangum Family Clinic	**APU ID:**	320886
Requested Date:	11/08/2024	**Expiration Date:**	12/09/2024
Customer No:	27384	**Created by:**	Tongchangya Athena

Prepared For:(Entity requesting work order)

Entity Requesting Work Order:	Mangum Family Clinic
Address:	118 S. louis Tittle,
City:	MANGUM
State:	OK
Zip:	73554
Contact Name:	Leslie Desmet (Analyst)
Phone:	918-857-2703
E-mail:	ldesmet@chmcok.com

Send Invoice To:

Paying Entity Name:	Mangum Family Clinic
Address:	118 S. louis Tittle,
City:	MANGUM
State:	OK
Zip:	73554
Contact Name:	Leslie Desmet (Analyst)
Phone:	918-857-2703
E-mail:	ldesmet@chmcok.com

Project ID:	2080206

Task Description	**Qty**	**Rate**	**Cost**
Interfaces - Lab or Radiology Bi-Directional (No Hub Contract). Lab results & orders with TruBridge EHR (formally known as CPSI/Evident)	1.0	$5,000.00	$5,000.00
		Amount	$5,000.00
		Total Amount	$5,000.00
Note: Quoted price subject to change if not signed prior to WO expiration date.			
Additional Notes:			

Cancellation Terms - If project is terminated:

Prior to any work being completed - A full refund will be issued.
Partial work has been completed, interface not yet installed - A 50% refund will be issued.
Interface has been installed - No refund will be issued.

Project Management Fees:

$750 per day (Project Management fees will be billed as incurred over the course of the Implementation until the applicable project(s) is/are Live. One day of Project Management is equivalent to 8 hours). i.e. Project Management Fees, will be billed monthly as incurred.

Item 10.

Maintenance Fee:

Maintenance Fee is calculated as 18% percentage of the One-Time Configuration Fee(s) as listed above. Maintenance fee to be billed annually until interface is shut down.

eCW Acknowledgement:

I have the authority to prepare this Work Order on behalf of eClinicalWorks. Upon receipt of a fully signed Work Order, this Work Order shall bind eClinicalWorks to the terms set forth herein.

Signed By Athena Tongchangya on 11/08/2024 11:28 AM

Work Order Sign Off:

Agreement:
OWNERSHIP AND PROPRIETARY RIGHTS. Customer may not attempt to sell, sublicense, lease, permit, rent or transfer in any way whatsoever the Software. Customer agrees that it will not, at any time, without the prior written consent of eClinicalWorks, decompile, disassemble or reverse engineer any software included within the Software, including without limitation the applications, to develop functionally similar to the Software or permit any third party to do any of the foregoing. Customer agrees to not grant access to any third party for any purpose without the prior written consent of eClinicalWorks.
OWNERSHIP OF DATA. All the patient demographics and medical records created by this Software will be solely owned by the Customer.
PAYMENT TERMS. Client will be invoiced upon receipt of Signed Work Order or Purchase Order. Payment is due in full within 30 days of invoicing. Undisputed invoices not paid by due date will be assessed 1.5% finance charges monthly. Invoices may include State and Local Sales Tax. Interface Installation will not occur without payment.

Acknowledgement:
I, the undersigned, having authority to approve these charges have agreed to the amount listed above and understand that this Work Order is a binding contractual agreement. I hereby accept this Work Order. I understand that checking this constitutes a legal signature confirming that I acknowledge and agree to the above Terms of Acceptance.

Authorized Representative Name:
Organization Name:
Date of Execution:

Comments :

Item 10.

Hospital Vendor Contract Summary Sheet

1. ☒ **Existing Vendor** ☐ **New Vendor**

2. **Name of Contract:** TruBridge

3. **Contract Parties: TruBridge/MRMC**

4. **Contract Type Services: IT Services**

5. **Impacted Hospital Departments:** Laboratory and Clinic

6. **Contract Summary:** This agreement is for a Bidirectional interface between TruBridge and eClinicalWorks. This will allow laboratory results to flow over to eClinicalWorks.

7. **Cost: $0**

8. **Term:** Previous TruBridge Agreement

9. **Termination Clause:** None

10. **Other:** Currently the staff at the clinics must research information in both systems. This allows results to be missed when ordered from eClinicalWorks and completed in TruBridge.

TruBridge®

Interface Performance Expectations

Third Party System: eClinicalWorks

Revised: November 8, 2024

In response to the hospital's request, TruBridge has performed a preliminary level of effort review of an interface between the software provided by TruBridge and the third-party system indicated above. The attached Interface Performance Expectations have been developed by TruBridge to reflect the communication protocols and functionality of the proposed interface. To ensure a clear understanding of the interface to be delivered by TruBridge, we require that representatives of the hospital review the attached performance expectations and provide confirmation of your agreement with interface communication protocols and functionality by signing below.

Please note that both this signed document and an order for the interface must be received by TruBridge before we will begin any additional development efforts as may be needed to deliver the interface.

However, it is understood that

1. the signing of this document **only** signifies agreement with the Interface Performance Expectations;
2. signing by the hospital **does not** obligate the hospital to order the proposed interface;

Hospital Name:____
(Print Clearly)

Hospital Location (City/State):______________________________

Hospital

By: ____________________________
(Authorized Signature)

Name: __________________________
(Printed)

Title: ___________________________

Date: ___________________________

TruBridge®

Interface Performance Expectations

Third Party System: eClinicalWorks

Revised: November 8, 2024

- Interface functionality includes:
  Inbound to TruBridge EHR – Laboratory orders (HL7 ORM message)
  Outbound from TruBridge EHR – Lab Results (HL7 ORU message)

- Data will be transmitted utilizing TCP/IP communications. TruBridge will be configured as the client for sending data. TruBridge will act as TCP/IP server when receiving data. HL7 Minimal Lower Layer Protocol will be followed for data framing. TruBridge expects to receive HL7 message acknowledgements from the receiving application.

- The proper functionality of this interface is dependent upon the facility being on the latest version of TruBridge EHR software. Modifications to the HIS programs are limited to the current software release and update.

- TruBridge EHR is ONC-ACB certified to the 2015 certification edition. Any interface transmitting data to meet Promoting Interoperability Program measures will be configured in HL7 v2.5.1 only.

- TruBridge will install HL7 unidirectional and bidirectional interfaces using version 2.5.1 unless otherwise noted prior to interface implementation.

- The interface functionality outlined in this PE does not include documents from TruBridge EHR Electronic File Management, Electronic Forms or Notes applications. Each of these applications requires a separate interface feed from TruBridge.

- Transmission of data via the interface:
  - > Only the last ten days of messages at any given time can be transmitted via the interface.
  - > Archived or historical data is ***not*** available for transmission via the interface.

- **Orders Inbound to Future Orders –**

  Receiving Inbound Future Orders:

  - > Upon receipt of the order message a search algorithm will be performed in TruBridge EHR for an existing person profile using parameters from the message, specifically SSN, last name, first name, and DOB. When a matching profile is found the Future orders will be associated to that existing profile. If no match is found a new profile will be created and the Future orders associated to the newly created profile. ***Based on the data received in the ORM message, there is the potential for an additional profile to be created for a patient with an existing profile in the TruBridge EHR Master Patient Index (MPI) if an exact match to the data on the HIS is not transmitted.***
  - > Patient guarantor information sent in the order message will be handled as follows:
    - o If a new person profile is created for the patient, the guarantor will be added to the new profile.
    - o If a person profile match is found and there is no existing guarantor on the profile, the guarantor will be added to the existing profile.
    - o If a person profile match is found and already contains a guarantor, the guarantor information from the order message will ***not*** update or replace existing guarantor information.

Interface Performance Expectations

Third Party System: eClinicalWorks

Revised: November 8, 2024

Releasing Future Orders Upon Patient/Specimen Arrival:

> When a patient or a sample arrives at the facility, if orders are available for processing the “Future orders” option will appear on the Person Profile and existing patient accounts associated with that profile. The orders can be released from the Person Profile, Patient Census, or Ancillary Department Patient Function Screen options. ***Facilities will be responsible for incorporating new procedures within their registration processes to check for future orders, for applicable patient types, on the person profile or patient account prior to following normal patient registration and order entry processes. Unprocessed future orders will automatically purge one year from the date they are received.***
- From the Person Profile the “Future orders” option is selected taking the user to the list of available future orders. Once orders are selected for release the user is then taken through the steps of creating a new patient visit to which the orders will be applied.
- From an existing patient account selecting the “Future orders” option, from either Census or Ancillary Patient Functions screens, will allow the user to select future orders to be released to that existing patient account.
- The Future Orders functionality does ***not*** support the release of orders from different ordering providers to a single patient account. Multiple orders received for the same patient must have the same ordering provider to be released to the same patient account.

> Departments are not notified of orders received via the interface until they are released through the Future Orders option from Person Profile, Patient Census, or Ancillary Department Patient Function Screen.

> Future orders that have been released to the ancillary department can be canceled and returned to the Unreleased Future Orders queue provided that the order has not yet been collected.

- **Processing Data Received with Inbound Orders**:

> The TruBridge EHR Person Profile, including guarantor and insurance information, will only be updated with the first order message received for the same date. The first order received on subsequent service dates will update the person profile.

> Patient insurance information sent in the order message will be uploaded to the person profile in the order in which it is received in the message. Any existing insurance information is not updated or removed.

> Diagnosis codes are ***not*** automatically uploaded to the Medical Record Grouper application. Within the Medical Record Grouper, a manual release is required to Insert Order Reason or Insert from Medical Necessity.

> Medical necessity checks and ABN is supported with the Future Orders interface ***(financial class required for Medical Necessity checks):***
- If diagnosis codes are provided in the HL7 ORM message, this information will be automatically uploaded to the medical necessity screen.
- If diagnosis codes are ***not*** provided in the HL7 ORM message, when the order is released to a patient visit the user will be prompted to enter a diagnosis code on the Medical Necessity screen where the check will occur.

> The TruBridge EHR item number (HL7 ORM message field OBR-4.1 procedure code) is required for the test(s) to be ordered.

> Repeat or recurring (standing) orders will be created by the interface only once; additional orders will need to be created manually or sent as separate order messages.

TruBridge®

Interface Performance Expectations

Third Party System: eClinicalWorks

Revised: November 8, 2024

> The interface can accept multiple orders (OBR segments) for a single patient per HL7 ORM message.

> Incoming orders should be identified by a diagnostic service. By default, orders are identified as "LAB" using HL7 field OBR-24 (diagnostic service section).

> TruBridge can receive order entry questions or notes in NTE segments (preferred) or OBX segments following the OBR segment. TruBridge does not utilize codes in OBX-3.1 for ask at order entry (AOE) questions.
  - o A maximum of four AOE NTE or OBX segments can be received for lab orders.
  - o A maximum of three AOE NTE or OBX segments can be received for rad orders.
  - o It is recommended that AOE questions in the third-party system match the existing set-up in TruBridge EHR as AOE questions or comments received from a third-party vendor will overwrite any existing AOE question(s) in the TruBridge software item setup for the patient order received.

> For orders received through the interface, TruBridge can save the third-party order or requisition number to return with results.

- **Functionality not supported with Inbound Orders:**

  > Orders uploaded via the interface are designed to coordinate with the level of care of patients treated in an outpatient "clinic" setting only. Inpatient orders are not in scope with this project.

  > The interface ***cannot*** upload a TruBridge EHR Contract Code to an existing profile or a new profile that may be created by the interface. When required, the facility will be responsible for manually entering a contract code onto the correct patient account.

  > The interface ***cannot*** upload or flag accounts with bill type information, i.e. Client Bill, Third Party Bill, or Patient Bill.

  > The interface ***cannot*** accept order updates or cancellations to existing orders with this interface.

  > Orders uploaded via an interface do not update TruBridge EHR scheduling applications.

  > "STAT" order notifications are not supported with this interface.

  > Orders uploaded via the interface are not assigned a status of "signed" in TruBridge EHR.

- **Lab Results Outbound from TruBridge EHR –**

  > Lab result results are sent in HL7 ORU messages and may include the following segments: MSH, SFT, PID, PD1, NK1, PV1, PV2, AL1, DG1, GT1, ACC, ORC, OBR, TQ1, OBX, NTE, and SPM. TruBridge can filter segments based on third-party system needs, if required.

  > TruBridge can include the third-party order or requisition number and patient identifier with results if the order was originally received through the interface from the third party. TruBridge cannot return the third-party patient identifier or the order/requisition number with reflex or add-on orders.

  > Lab results may include both discrete and non-discrete text data sent in HL7 ORU messages. For the transmission of discrete reference lab and microbiology results please see the **Notes below.

  > TruBridge will send corrections of single test results that are part of an ordered panel, i.e. CBC. A status of "C" will be applied to OBX.11 for the corrected test(s). The entire panel will be included in the transmission.

TruBridge®

Interface Performance Expectations

Third Party System: eClinicalWorks

Revised: November 8, 2024

> By default, TruBridge EHR order codes (item number) and test codes will be sent in OBR-4 and OBX-3, respectively, of the HL7 ORU message. TruBridge EHR utilizes the test name as both the test code and test description. Example: OBX|1|NM|Hemoglobin^Hemoglobin|…

> When available, the applicable LOINC codes along with the local order and test codes will be sent in the HL7 message.
  - The coding systems for local and LOINC codes will be identified in the appropriate HL7 OBR-4 and OBX-3 component fields.
  - It is the facility's responsibility to ensure LOINC codes are loaded in the appropriate tables within TruBridge EHR software applications. ***Note: LOINC codes are not available at the test level (OBX-3) with results sent as non-discrete text.***

> Results can be transmitted automatically when they are completed. Results can also be re-sent using manual send options within the TruBridge EHR software applications. Retransmission of results will contain all tests for that order.

> Only final/verified results will be transmitted unless otherwise specified by the facility.

NOTES:
Modifications to third-party reference lab interfaces and/or Microbiology analyzer interfaces to accommodate discrete and coded results will not automatically apply to outbound lab result interfaces.

To enable discrete/coded lab results to be transmitted from TruBridge EHR to existing lab result-receiving vendors, the facility is encouraged to coordinate discussions with those vendors and contact TruBridge to initiate the appropriate modifications to those interfaces.

When changes are made to begin sending discrete/coded reference lab results to a downstream vendor all downstream interfaces will receive discrete/coded reference lab results.

Modifications to accommodate discrete/coded microbiology results can be made per individual interface.

- Sample messages from the facility's TruBridge EHR software can be provided after the scheduled implementation begins and messages are being generated.

- Translations may be required for some table-driven fields in TruBridge EHR, such as race, relationship, etc.
  > For any translations not performed by the third-party vendor, the facility will need to provide TruBridge with a one-to-one cross-reference of TruBridge EHR codes to third-party codes prior to development of the interface.
  > The cross-reference file provided can be an Excel file or comma-delimited text file. Once the initial translation tables are created, the facility will be responsible for any future maintenance to the tables.

- Messages may be filtered by physician, service code and/or patient type. When filtering by physician, it is TruBridge's recommendation that a facility-maintained translation table be set up for the facility to add or remove physicians as needed. ***When TruBridge is asked to perform result filtering based***

Interface Performance Expectations

Third Party System: eClinicalWorks

Revised: November 8, 2024

on physician, notification to TruBridge is required when a physician's privileges are inactivated in the third-party system. Otherwise, results will continue to be sent as per the original configuration.

- As TruBridge strives to meet the changing needs of the healthcare industry and the complexities required with interoperability, future enhancements to the software may necessitate modifications to existing facility interfaces. We encourage all facilities to plan accordingly for the potential of longer development time, supplementary input from parties involved and additional fees. TruBridge is not responsible for any third-party vendor costs that may be incurred for interface changes.

- The above requirements meet the preliminary needs for the interface. This initial sign-off is needed prior to development of the interface. Relatively minor changes during development are permitted if the third-party and TruBridge both agree that it will not impact development resources/timelines and implementation target dates. Please note that changes outside the scope of this initial interface performance expectation will require review for level of effort and may necessitate an additional quote.

TruBridge, Inc.

System Solution

for

MANGUM REGIONAL MEDICAL CENTER

Submitted by:	**Submitted to:**
Jennifer Hester **Inside Account Management**	**Leslie DeSmet**

Date Submitted: November 8, 2024

MANGUM REGIONAL MEDICAL CENTER

INTERFACE MANAGEMENT SYSTEM

Interface

```
Bidirectional Interface - eClinicalWorks
Includes: Inbound Lab Orders
          Outbound Lab Results
```

INTERFACE TOTAL

Testing to begin with facility 90-days from order placement. Once an order is placed and timeline confirmed, our assigned analyst will work with the client and vendor to complete the project in a timely manner. If there is no client and/or vendor engagement for a period of ten(10) business days, the assigned contacts for the project will be alerted and the project will be monitored for signs of progress. If after ten additional business days there is still no client/vendor engagement, the project will be flagged as inactive, removed from the assigned analyst and returned to a resource coordinator to discuss a future timeline for the project.

MANGUM REGIONAL MEDICAL CENTER
SUMMARY - INTERFACE MANAGEMENT SYSTEM

Interface Management System Bidirectional Interface - eClinicalWorks	**$0**
SYSTEM PRICE	**$0**
TOTAL	**$0**

Proposal is based on Performance Expectation (PE) provided for review.
Signed Performance Expectation required prior to order placement.
Testing to begin with facility 90 days after order placement.
If on-site assistance is requested or becomes necessary, expenses
will be billed as incurred.

Hardware prices in this proposal will remain valid for a
period of 30 days. All other prices will remain valid
for 90 days.

careLearning
eLearning. Real-World Advantages.

Third Party Content Usage Agreement

Purpose

Your organization has requested courses from ____________________________, a 3rd Party Content Provider, be placed on the careLearning Learning Management System (LMS). Courses provided by a 3rd Party Content Provider are ultimately the responsibility of the 3rd Party Content Provider. Failure to comply with the steps outlined in the 3rd Party Content policy of the careLearning Product Guide may result in the courses not functioning properly on the LMS. careLearning is not responsible for any costs incurred if the organization has failed to follow this policy.

The process for purchasing, managing, and utilizing courses from a 3rd Party Content Provider differs from careLearning's typical course practices. This agreement is designed to outline these processes.

Procedure

1. careLearning will generate an invoice for the one-time, non-refundable integration fee of $500 per 3rd Party Content Provider for the organization. NOTE: Courses secured during the organization's LMS implementation and courses procured from RQI Partners (HeartCode, RQI, NRP) are excluded from the integration fee.
2. The organization is responsible for obtaining the courses from the 3rd Party Content Provider, providing the SCORM 1.2 or AICC course files with accompanying spreadsheet to careLearning, testing the courses, and reporting the results.
3. careLearning is responsible for providing access to a shared folder for receipt of the course files and accompanying spreadsheet, installing and setting up the courses for testing and usage, and providing instructions for adding the courses to the organization's Administrative Management System (AMS).
4. The organization agrees to inform careLearning when the 3rd Party Content Provider course(s) have been revised/updated or can be retired from the LMS due to the termination of the license with the 3rd Party Content Provider.
5. All 3rd Party Content will be deleted from the LMS upon termination of the organization's license with the 3rd Party Content Provider or of the organization's careLearning LOU (whichever comes first).

Term and Termination

This agreement shall be signed upon the request of courses from a 3rd Party Content Provider be placed on the LMS and shall be extended between the parties (careLearning and the organization) for said time.

____	____________________
Organization Name	Date
____	_________________________________
Signature	Title

Hospital Vendor Contract Summary Sheet

1. ☒ **Existing Vendor** ☐ **New Vendor**

2. **Name of Contract: Tecumseh Oxygen & Medical Supply**

3. **Contract Parties: Tecumseh Oxygen & Medical Supply/MRMC**

4. **Contract Type Services: Service Agreement**

5. **Impacted Hospital Departments:** Nursing

6. **Contract Summary:** This agreement is to provide Durable Medical Equipment to the facility to fulfill patient care needs. This equipment will then be charged to the facility on a daily basis. The DME will provide equipment in good working order.

7. **Cost: Based on equipment usage**

8. **Term:** 1-year then annual automatic renewal

9. **Termination Clause:** 30-day written notice

10. **Other:** The total cost is $500.00 but this amount is split among the 5 hospitals.

AGREEMENT FOR THE PROVISION·& MAINTENANCE OF DURABLE MEDICAL EQUIPMENT

Tecumseh Oxygen & Medical Supply

This agreement is made and entered into this ______ day of ____________ 2024, by and between **Tecumseh Oxygen & Medical Supply** (hereinafter referred to as "DME") and ________________________ (hereinafter referred to as "CLIENT"). The following shall be deemed an agreement between CLIENT and DME for the provision of various items of durable medical equipment and maintenance specifically related to same.

WHEREAS, DME is a durable medical equipment provider, is willing to make services available to CLIENT patients;

NOW THEREFORE, in consideration of the agreement set forth herein, the parties hereby agree as follows:

A. RESPONSIBILITIES OF DME. DME shall:

1. Deliver equipment by next business day of the request.

2. Assure, on a continuing basis that all equipment is in good clean condition and working order.

3. Instruct the patient and/or caregiver(s) on the safe and intended use of such equipment.

4. Pickup the equipment according to arrangement made with the CLIENT.

5. Pro-rate charges on a daily basis, per patient, according to fee schedule.

6. Develop preventive maintenance in accordance with DME policy pertaining to the equipment.

7. Notify CLIENT if care conference is necessary concerning patient's equipment.

8. Submit monthly statements to CLIENT for authorized patients at the end of each month. Include the patient's name, equipment ordered, fee, delivery date and pick-up date, if applicable.

9. Provide services to all patients regardless of diagnosis, race, age, sex, religion, national origin, disability, sexual preference and marital status.

10. If services provided under this agreement have an aggregate value of $10,000.00 or more over a twelve month period, DME shall, until the

expiration of four years after the furnishing of such services, make available upon written request by the Secretary of Health and Human Services, Comptroller General of the United States, or by any of the Secretaries of the Comptroller Generals duly authorized representative this agreement and books, documents and records of DME that are necessary to verify the nature and extent of the cost of services provided.

11. DME agrees to maintain high standards of confidentiality for information relating to this Agreement including, but not limited to, information concerning CLIENT patients, in accordance with federal and state laws and specifically as specified in “Addendum A”. DME acknowledges that all material and information including; but not limited to, descriptions of the arrangements between DME and CLIENT hereunder and Plans of Care which have or will come into the possession of DME in connection with the performance of the terms and conditions of this Agreement, consist of confidential and proprietary data, whose disclosure to or use by third parties will be damaging to CLIENT. DME agrees to hold such material and information in strictest confidence, and not to make use thereof except as required by applicable Federal or State Law and as expressly set forth in this Agreement.

12. DME at all times shall maintain liability insurance, including products’ liability coverage, in the amount of One Million and Noll 00 Dollars ($1,000,000.00) per occurrence, and Three Million and Noll 00 Dollars ($3,000,000) annual aggregate and will provide evidence of such insurance to CLIENT. CLIENT assumes no responsibility to maintain or provide general liability insurance or workers’ compensation insurance for DME or its agents, servants, and employees. DME agrees·to hold CLIENT harmless and to indemnify CLIENT from any and all liability, costs, expenses, including attorney’s fees and court costs, which arise or are incurred by CLIENT because of any act or omission by CLIENT, its agents, servants, and employees. CLIENT shall furnish evidence satisfactory to DME that it has obtained comprehensive general liability insurance covering any negligence of CLIENT or its agents or employees in connection with its operation.

13. DME agrees to indemnify and hold harmless CLIENT from any and all liability, loss, expenses, including reasonable attorney’s fees, and claims for damages or injury arising from negligence or intentional acts or omissions by DME, its agent, servants, employees, or arising from any breach of default on the part of DME in the performance of this Agreement. DME, upon reasonable notice from CLIENT, shall assume the defense, at the expense of DME, or such action or proceeding with counsel reasonably satisfactory to CLIENT.

B. RESPONSIBILITIES OF CLIENT. CLIENT shall:

1. Evaluate and assess CLIENT patient equipment needs.

2. Coordinate and supervise the care plans of the CLIENT patient.

3. Develop, review and revise the care plans of CLIENT patients.

4. Address care conferences by telephone on·an as needed basis, since the majority of CLIENT patient's equipment needs are short-term.

5. Telephone equipment request to DME giving patient's name and other information only to the extent required to insure prompt and safe delivery of equipment/supplies, equipment needed, date and preferred time of delivery.

6. Record all equipment requests in CLIENT DME log.

7. Notify DME within 24 hours following a patient discharge for a pickup date and time. If discharge occurs on a weekend or holiday, CLIENT will notify DME by the end of the next regular business day.

8. Communicate any equipment problems promptly.

9. Pay DME within 30 days of receipt of invoice.

10. CLIENT agrees to indemnify and hold harmless DME from any and all liability, loss, expenses, including reasonable attorney's fees, and claims for damages or injury arising from the negligent or intentional acts or omissions by CLIENT, its agents, servants and employees, or arising from any breach of default on the part of CLIENT in the performance of this Agreement. CLIENT, upon reasonable notice from DME shall assume the defense, at the expense of CLIENT, of such action or proceeding with counsel reasonable satisfactory to CLIENT.

C. JOINT RESPONSIBILITIES OF DME AND CLIENT. DME and CLIENT also agree to the following:

1. All notices shall be deemed received on the day personally delivered, or on the second day after mailing, certified or registered. Return receipt requested, to the address reflected on the signature page, or to such other address as the parties shall respectively by notice designate.

2. DME and CLIENT are separate and independent entities. Except as specifically provided in this Agreement, neither party is granted any express or implied right or authority by the other party to assume or create any obligation or responsibility on behalf of or in the name of the other party or to bind the other party in any manner or thing whatsoever. Each

party retains its own authority and responsibility for its respective organizations. Nothing herein shall be construed as creating a partnership or joint venture between CLIENT and DME.

3. This Agreement shall be governed by and interpreted in accordance with, the laws of the State of Oklahoma, without giving effect to its conflict of laws provisions. _________ County, Oklahoma, shall be the sole and exclusive venue for any arbitration, litigation, special proceeding or other proceeding as between the parties that may be brought under, or arise out of, this agreement.

4. The initial term of this Agreement shall be one year from the effective date. After the completion of the initial one (1) year term, this Agreement shall continue automatically for additional one (l) year terms unless notice of termination is given by either party in writing on or before ninety (30) days prior to the termination date. The extended term shall be subject to the same terms and conditions as set forth in this Agreement except for any mutually agreed written amendments, including any change of hourly payments. Either party may terminate this Agreement at any time without cause by providing the other party with thirty (30) day advance written notice of intent to terminate.

5. This agreement embodies the entire agreement between the Parties and supersedes all prior agreements and understandings, if any, relating to the subject matter hereof. and this Agreement may be amended only by and instrument in writing executed jointly by an officer duly authorized by the board of directors of the respective Parties.

6. This Agreement may not be assigned by either party without the prior written consent of the other party.

7. If any provision of this Agreement, or the application there of to any person or circumstance, is held to be illegal, invalid, or unenforceable for any reason, such illegality, invalidity, or unenforceability shall not affect any other provision of this Agreement that can be given effect in the absence of the illegal, invalid, or unenforceable provision of application. To this end, all provisions of this Agreement are declared to be severable.

8. Until the expiration of four years after the furnishing of services pursuant to this Agreement, the DME and CLIENT shall make available, upon written request of the Secretary of the Department of Health and Human Services, the Comptroller General of the United States, or another duly authorized representative, this Agreement and the books, documents, and records that are necessary to certify the nature and the extent of the cost of services provided pursuant to this Agreement.

[SIGNATURE PAGE TO FOLLOW]

Item 14.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed effective the date and year first mentioned in this Agreement.

______________________________	Tecumseh Oxygen & Medical Supply
By: ___________________________	By: ___________________________
Name: _________________________	Name: _________________________
Title: __________________________	Title: __________________________
Date: __________________________	Date: __________________________

Addendum A
Business Associates Agreement

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is made as of the _________________, 2024, ("Effective Date") by and between _______________________ ("Covered Entity") and ___________________, ("Business Associate").

RECITALS

A. Covered Entity and Business Associate are parties to an Agreement for the Provision & Maintenance of Durable Medical Equipment dated ___________, 2024 (the "Agreement") pursuant to which Business Associate provides certain services to the Covered Entity and, in connection with those services, the Covered Entity discloses to Business Associate certain individually identifiable protected health information ("PHI") that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the American Recovery and Reinvestment Act of 2009 ("ARRA") and the associated regulations, 45 CFR Parts 160 and 164 (the "Privacy Rule"), as amended from time to time.

B. The parties desire to comply with the HIPAA standards for the privacy and security of PHI of patients of the Covered Entity.

NOW, THEREFORE, for and consideration of the recitals above and the mutual covenants and conditions contained herein, the parties enter into this Agreement to provide a full statement of their respective responsibilities.

SECTION 1 - Definitions

1.01 Reference to HIPAA Rules.

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

1.02 Specific definitions.

(a) Business Associate. "Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _______________________.

(b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean ________________________.

(c) HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

SECTION 2 - Obligations and Activities of Business Associate

2.01 Performance of Services Agreement. Business Associate agrees to not use or disclose PHI other than as permitted or required by the Services Agreement or as required by law.

2.02 Safeguards for Protection of PHI. Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Services Agreement and this Agreement.

2.03 Mitigation of Harm of Unauthorized Use or Disclosure. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

2.04 Reporting of Unauthorized Use or Disclosure. As soon as practicable, but in no event later than ten (10) days, Business Associate agrees to report to Covered Entity in writing any use or disclosure of PHI not provided for by the Services Agreement or this Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Such report shall contain:

(a) A brief description of what happened, including the date of the unauthorized access or use of PHI and the date of the discovery of the unauthorized access or use of PHI;

(b) A description of the type of unsecured PHI that was involved in the unauthorized access or use;

(c) Any recommended steps the individual whose PHI was inappropriately disclosed should take to protect themselves from the potential harm; and

(d) A brief description of what the Business Associate is doing to investigate the unauthorized access or use of PHI.

Business Associate will report such incidents to the Covered Entity's Privacy Officer. Business Associate will, subject to the approval of the Covered Entity, provide breach notifications to affected individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the Covered Entity. If the Covered Entity elects to be responsible for all required notifications, the Business Associate shall reimburse the Covered Entity for the costs associated with the notifications. Such costs will be paid to Covered Entity by Business Associate within thirty (30) days of receipt of an itemized invoice from the Covered Entity.

2.05 Use of Subcontractors. Business Associate agrees, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to contract with any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate whereby such subcontractors agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

2.06 Access to PHI. Business Associate shall make available PHI in a designated record set to the Covered Entity, or as directed by the Covered Entity to an individual or the individual's designee, for inspection and copying within ten (10) days of a request by Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.524.

2.07 Amendment by Business Associate. Business Associate agrees to make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526, within thirty (30) days of receipt of a request from Covered Entity.

2.08 Documentation of Disclosures. Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity, or as directed by the Covered Entity, to an individual, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528. Business Associate shall provide such information to the Covered Entity within ten (10) days of a request by Covered Entity.

2.09 Compliance with Patient Right Provisions of Privacy Rule. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

2.10 Opportunity to Object. Business Associate agrees that, if it has a legal obligation to disclose any PHI, it will notify the Covered Entity as soon as reasonably practical after it learns of such obligation, and in any event within a time sufficiently in advance of the proposed release date such that Covered Entity's rights would not be prejudiced, as to the legal requirement pursuant to which it believes the PHI must be released. If the Covered Entity objects to the release of such PHI, Business Associate will allow the Covered Entity to exercise any legal rights or remedies the Covered Entity might have to object to the release of PHI, and Business Associate agrees to provide such assistance to Covered Entity, at Covered Entity's expense, as Covered Entity may reasonably request in connection therewith.

2.11 Access to Books and Records. Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

SECTION 3 - Permitted Uses and Disclosures by Business Associate

3.01 Services Agreement. Business Associate may use or disclose PHI as necessary to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate the HIPAA Rules if done by the Covered Entity.

3.02 Other Permitted Uses and Disclosures.

(a) Business Associate may use or disclose PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c).

(b) Business Associate may use or disclose PHI as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for PHI consistent with the Covered Entity's minimum necessary policies and procedures.

(d) Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Covered Entity, except for the specific uses and disclosures set forth below.

SECTION 4 – Obligations of Covered Entity

4.01 Inform of NPP. The Covered Entity shall notify Business Associate of any limitation(s) in the Covered Entity's notice of privacy practices under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

4.02 Notification of Revocation. The Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

4.03 Notification of Restriction. The Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4.04 Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the HIPAA Regulations if done by Covered Entity, except as permitted pursuant to the provisions of Sections 2(b), 2(c), 2(d) and 2(e) of this BAA.

4.05 Notice of Amendments. Covered Entity shall notify Business Associate of any amendments made by an Individual to Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.526, to the extent that Business Associate relies or could foreseeably rely on such amended Protected Health Information. Covered Entity shall provide such notice no later than fifteen (15) days prior to the effective date of the change.

4.06 Notice of Potential Problems. Covered Entity shall provide notice to Business Associate of any pattern of activity or practice of Business Associate that Covered Entity believes constitutes a material breach or violation of Business Associate’s obligation under the Underlying Agreement or Agreement or other arrangement within five (5) calendar days of discovery and shall meet with Business Associate to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

4.07 Notification of Security Incidents. Covered Entity shall immediately notify Business Associate of any Security Incidents or other security issues/concerns with Covered Entity’s environment, including, but not limited to, ransomware, where Business Associate performs services. Provided, however, that Covered Entity shall not be required to report an immaterial incident consisting solely of an unsuccessful attempt to improperly access Electronic PHI that is stored in an information system under its control.

4.08 Privacy/Security. Covered Entity shall ensure that it follows all generally accepted industry practices for privacy and security of its systems, including, but not limited to, the requirement for complex passwords, unique user ids, password resets, and the timely granting of systematic access and termination of said access when notified. Further, Covered Entity shall only provide to Business Associate access to the minimum necessary PHI required to perform the services under the Agreement.

SECTION 5 - Term and Termination

5.01 Term. This Agreement shall become effective on the Effective Date and shall terminate on the same date that the Service Agreement terminates, or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner. In addition, certain provisions and requirements of this Agreement shall survive its expiration or other termination in accordance with Section 7.04 herein.

5.02 Termination for Cause. The Covered Entity may immediately terminate this Agreement and any related Service Agreement if the Covered Entity makes the determination that the Business Associate has breached a material term of this Agreement, provided an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Service Agreement if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity, except that the Covered Entity will immediately terminate this Agreement and the Service Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

5.03 Obligations of Business Associate Upon Termination. Upon termination of this

Agreement for any reason, Business Associate, with respect to PHI received from the Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(a) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(b) Return to the Covered Entity or, if agreed to by the Covered Entity, destroy, the remaining PHI that the Business Associate still maintains in any form;

(c) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

(d) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section 3.02(e) and (f) above which applied prior to termination;

(e) Return to Covered Entity or, if agreed to by Covered Entity, destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities; and;

(g) Obtain or ensure the destruction of PHI created, received, or maintained by any of the Business Associate's subcontractors.

SECTION 6 – Indemnification and Disclaimer

6.01 Indemnification. Business Associate shall indemnify, defend and hold Covered Entity and its [parent corporation] and affiliates, their directors, officers, agents, servants, and employees (collectively "the Indemnitees") harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, incurred by the Indemnitees and relating to or arising out of breach or alleged breach of the terms of this Agreement, or a violation of the HIPAA Rules, by Business Associate.

Covered Entity shall indemnify, defend and hold Business Associate and its parent corporation and affiliates, their directors, officers, agents, servants, and employees (collectively "the Indemnitees") harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, incurred by the Indemnitees and relating to or arising out of breach or alleged breach of the terms of this Agreement, or a violation of the HIPAA Rules, by Covered Entity.

6.02 Disclaimer. COVERED ENTITY MAKES NO WARRANTY OR REPRESENTATION THAT COMPLIANCE BY BUSINESS ASSOCIATE WITH THIS AGREEMENT OR THE HIPAA RULES WILL BE ADEQUATE OR SATISFACTORY FOR BUSINESS ASSOCIATE'S OWN PURPOSES. BUSINESS ASSOCIATE IS SOLELY RESPONSIBLE FOR ALL DECISIONS MADE BY BUSINESS ASSOCIATE REGARDING THE SAFEGUARDING OF PHI.

SECTION 7 - Miscellaneous

7.01 Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

7.02 Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties.

7.03 Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

7.04 Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2.01, 2.02, 2.03, 2.04, 2.10, 5.03 and 6.01, to the extent applicable, shall survive termination of this Agreement indefinitely. In addition, Sections 2.06 and 2.07 shall survive termination of this Agreement, provided that the Covered Entity determines that the PHI being retained pursuant to Section 5.03 herein constitutes a Designated Record Set.

7.05 No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

7.06 Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party’s address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.
If to Business Associate, to:

If to Covered Entity, to:

Each party named above may change its address and that of its representative for notice by the giving of notice of the change in the manner provided above.

7.07 Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies of this document shall be deemed to be originals.

7.08 Governing Law. The laws of the State of Oklahoma shall govern the interpretation of this Agreement and shall apply in any lawsuit or other dispute arising out of this Agreement, without regard to conflict of laws provisions.

IN WITNESS WHEREOF, the parties have hereunto set their hands effective the Effective Date first above written.

COVERED ENTITY

By: ______________________________

Print Name: ______________________

Print Title: ______________________

Date: _____________________________

BUSINESS ASSOCIATE

By:_________________________________

Print Name: ________________________

Print Title:__________________________

Date: ________________________________

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is made as of the 25 September, 2024, ("Effective Date") by and between **Mangum Regional Medical Center** ("Covered Entity") and **Sinor EMS**, ("Business Associate").

RECITALS

A. Covered Entity and Business Associate are parties to a certain agreement (the "Services Agreement") pursuant to which Business Associate provides certain services to the Covered Entity and, in connection with those services, the Covered Entity discloses to Business Associate certain individually identifiable protected health information ("PHI") that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the American Recovery and Reinvestment Act of 2009 ("ARRA") and the associated regulations, 45 CFR Parts 160 and 164 (the "Privacy Rule"), as amended from time to time.

B. The parties desire to comply with the HIPAA standards for the privacy and security of PHI of patients of the Covered Entity.

NOW, THEREFORE, for and consideration of the recitals above and the mutual covenants and conditions contained herein, the parties enter into this Agreement to provide a full statement of their respective responsibilities.

SECTION 1 - Definitions

1.01 Reference to HIPAA Rules.

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

1.02 Specific definitions.

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean **Sinor EMS**.

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean **Mangum Regional Medical Center**.

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

SECTION 2 - Obligations and Activities of Business Associate

2.01 Performance of Services Agreement. Business Associate agrees to not use or disclose PHI other than as permitted or required by the Services Agreement or as required by law.

2.02 Safeguards for Protection of PHI. Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Services Agreement and this Agreement.

2.03 Mitigation of Harm of Unauthorized Use or Disclosure. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

2.04 Reporting of Unauthorized Use or Disclosure. As soon as practicable, but in no event later than ten (10) days, Business Associate agrees to report to Covered Entity in writing any use or disclosure of PHI not provided for by the Services Agreement or this Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware. Such report shall contain:

(a) A brief description of what happened, including the date of the unauthorized access or use of PHI and the date of the discovery of the unauthorized access or use of PHI;

(b) A description of the type of unsecured PHI that was involved in the unauthorized access or use;

(c) Any recommended steps the individual whose PHI was inappropriately disclosed should take to protect themselves from the potential harm; and

(d) A brief description of what the Business Associate is doing to investigate the unauthorized access or use of PHI.

Business Associate will report such incidents to the Covered Entity's Privacy Officer. Business Associate will, subject to the approval of the Covered Entity, provide breach notifications to affected individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the Covered Entity. If the Covered Entity elects to be responsible for all required notifications, the Business Associate shall reimburse the Covered Entity for the costs associated with the notifications. Such costs will be paid to Covered Entity by Business Associate within thirty (30) days of receipt of an itemized invoice from the Covered Entity.

2.05 Use of Subcontractors. Business Associate agrees, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to contract with any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate whereby such subcontractors agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

2.06 Access to PHI. Business Associate shall make available PHI in a designated record set to the Covered Entity, or as directed by the Covered Entity to an individual or the individual's designee, for inspection and copying within ten (10) days of a request by Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.524.

2.07 Amendment by Business Associate. Business Associate agrees to make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526, within thirty (30) days of receipt of a request from Covered Entity.

2.08 Documentation of Disclosures. Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity, or as directed by the Covered Entity, to an individual, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528. Business Associate shall provide such information to the Covered Entity within ten (10) days of a request by Covered Entity.

2.09 Compliance with Patient Right Provisions of Privacy Rule. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

2.10 Opportunity to Object. Business Associate agrees that, if it has a legal obligation to disclose any PHI, it will notify the Covered Entity as soon as reasonably practical after it learns of such obligation, and in any event within a time sufficiently in advance of the proposed release date such that Covered Entity's rights would not be prejudiced, as to the legal requirement pursuant to which it believes the PHI must be released. If the Covered Entity objects to the release of such PHI, Business Associate will allow the Covered Entity to exercise any legal rights or remedies the Covered Entity might have to object to the release of PHI, and Business Associate agrees to provide such assistance to Covered Entity, at Covered Entity's expense, as Covered Entity may reasonably request in connection therewith.

2.11 Access to Books and Records. Business Associate agrees to make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

SECTION 3 - Permitted Uses and Disclosures by Business Associate

3.01 Services Agreement. Business Associate may use or disclose PHI as necessary to perform functions, activities, or services for, or on behalf of, the Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate the HIPAA Rules if done by the Covered Entity.

3.02 Other Permitted Uses and Disclosures.

(a) Business Associate may use or disclose PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c).

(b) Business Associate may use or disclose PHI as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for PHI consistent with the Covered Entity's minimum necessary policies and procedures.

(d) Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 CFR Part 164 if done by the Covered Entity, except for the specific uses and disclosures set forth below.

SECTION 4 – Obligations of Covered Entity

4.01 Inform of NPP. The Covered Entity shall notify Business Associate of any limitation(s) in the Covered Entity's notice of privacy practices under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

4.02 Notification of Revocation. The Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

4.03 Notification of Restriction. The Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4.04 Permissible Requests by Covered Entity. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the HIPAA Regulations if done by Covered Entity, except as permitted pursuant to the provisions of Sections 2(b), 2(c), 2(d) and 2(e) of this BAA.

4.05 Notice of Amendments. Covered Entity shall notify Business Associate of any amendments made by an Individual to Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.526, to the extent that Business Associate relies or could foreseeably rely on such amended Protected Health Information. Covered Entity shall provide such notice no later than fifteen (15) days prior to the effective date of the change.

4.06 Notice of Potential Problems. Covered Entity shall provide notice to Business Associate of any pattern of activity or practice of Business Associate that Covered Entity believes constitutes a material breach or violation of Business Associate's obligation under the Underlying Agreement or Agreement or other arrangement within five (5) calendar days of discovery and shall meet with Business Associate to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

4.07 Notification of Security Incidents. Covered Entity shall immediately notify Business Associate of any Security Incidents or other security issues/concerns with Covered Entity's environment, including, but not limited to, ransomware, where Business Associate performs services. Provided, however, that Covered Entity shall not be required to report an immaterial incident consisting solely of an unsuccessful attempt to improperly access Electronic PHI that is stored in an information system under its control.

4.08 Privacy/Security. Covered Entity shall ensure that it follows all generally accepted industry practices for privacy and security of its systems, including, but not limited to, the requirement for complex passwords, unique user ids, password resets, and the timely granting of systematic access and termination of said access when notified. Further, Covered Entity shall only provide to Business Associate access to the minimum necessary PHI required to perform the services under the Agreement.

SECTION 5 - Term and Termination

5.01 Term. This Agreement shall become effective on the Effective Date and shall terminate on the same date that the Service Agreement terminates, or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner. In addition, certain provisions and requirements of this Agreement shall survive its expiration or other termination in accordance with Section 7.04 herein.

5.02 Termination for Cause. The Covered Entity may immediately terminate this Agreement and any related Service Agreement if the Covered Entity makes the determination that the Business Associate has breached a material term of this Agreement, provided an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Service Agreement if Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity, except that the Covered Entity will immediately terminate this Agreement and the Service Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

5.03 Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from the Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(a) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(b) Return to the Covered Entity or, if agreed to by the Covered Entity, destroy, the remaining PHI that the Business Associate still maintains in any form;

(c) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

(d) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section 3.02(e) and (f) above which applied prior to termination;

(e) Return to Covered Entity or, if agreed to by Covered Entity, destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities; and;

(g) Obtain or ensure the destruction of PHI created, received, or maintained by any of the Business Associate's subcontractors.

SECTION 6 – Indemnification and Disclaimer

6.01 Indemnification. Business Associate shall indemnify, defend and hold Covered Entity and its [parent corporation] and affiliates, their directors, officers, agents, servants, and employees (collectively "the Indemnitees") harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, incurred by the Indemnitees and relating to or arising out of breach or alleged breach of the terms of this Agreement, or a violation of the HIPAA Rules, by Business Associate.

Covered Entity shall indemnify, defend and hold Business Associate and its parent corporation and affiliates, their directors, officers, agents, servants, and employees (collectively "the Indemnitees") harmless from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution, incurred by the Indemnitees and relating to or arising out of breach or alleged breach of the terms of this Agreement, or a violation of the HIPAA Rules, by Covered Entity.

6.02 Disclaimer. COVERED ENTITY MAKES NO WARRANTY OR REPRESENTATION THAT COMPLIANCE BY BUSINESS ASSOCIATE WITH THIS AGREEMENT OR THE HIPAA RULES WILL BE ADEQUATE OR SATISFACTORY FOR BUSINESS ASSOCIATE'S OWN PURPOSES. BUSINESS ASSOCIATE IS SOLELY RESPONSIBLE FOR ALL DECISIONS MADE BY BUSINESS ASSOCIATE REGARDING THE SAFEGUARDING OF PHI.

SECTION 7 - Miscellaneous

7.01 Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

7.02 Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties.

7.03 Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

7.04 Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2.01, 2.02, 2.03, 2.04, 2.10, 5.03 and 6.01, to the extent applicable, shall survive termination of this Agreement indefinitely. In addition, Sections 2.06 and 2.07 shall survive termination of this Agreement, provided that the Covered Entity determines that the PHI being retained pursuant to Section 5.03 herein constitutes a Designated Record Set.

7.05 No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

7.06 Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.

If to Business Associate, to:

Sinor EMS, Inc
Attn: Anne Lambeth, Privacy Officer
1101 Frisco Ave, Clinton, OK 73601

If to Covered Entity, to:

____
____
____

Each party named above may change its address and that of its representative for notice by the giving of notice of the change in the manner provided above.

7.07 Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies of this document shall be deemed to be originals.

7.08 Governing Law. The laws of the State of Oklahoma shall govern the interpretation of this Agreement and shall apply in any lawsuit or other dispute arising out of this Agreement, without regard to conflict of laws provisions.

IN WITNESS WHEREOF, the parties have hereunto set their hands effective the Effective Date first above written.

COVERED ENTITY	BUSINESS ASSOCIATE
By: ____________________	By: Anne Lambeth
Print Name: ____________________	Print Name: Anne Lambeth

Print Title: ____________________

Date: ____________________

Print Title: President / Privacy Officer

Date: 9/25/2024

Repetitive Wire/ACH Authorization Form

(Reoccurring wires/ACHs need to be approved at initiation or at any time a change/alteration is made to the initially approved wire/ACH)

☒ Initial

☐ Revised

Repetitive Wire/ACH Set Up

The following items have been included in the request:

1. Attach approved invoice/contract and supporting documentation to this form.
2. Attach explanation of why this payment cannot be paid by check.
3. Vendor documents/wiring instructions

Explain the Purpose of the Wire/ACH Change

Nuance Communications no longer accepts checks they only accept credit card payments or ACH

Reoccurring Amount of wire/ACH $202.00

Accounts Payable **Date**

Director Approval Repetitive Wire/ACH Transfers

☐ Wire instructions verification with vendor (please check)

☐ Confirmed no other payment options with vendor (please check)

Director of Finance or Hospital CFO **Date**

Wire Originator Signature
(Board Member/City Originator) **Date**