State Patrol Message Switching System (MSS) Modernization Project

MARCH 24, 2023

unisys

diverse™ COMPUTING

Demonstration and Presentation Schedule

01
8:30-8:40am
Introductions and Guidelines
10 minutes

02
8:40-9:00am
Product Approach and Overview
20 minutes

03
9:00-10:00am
Focused Demonstration
50 minutes

04
10:00-10:15am
Break
15 minutes

05
10:15-11:30am
Focused Demonstration
75 minutes

06
11:30-12:00am
Additional Topics
30 minutes

07
12:00-1:00pm
Lunch
60 minutes

08
1:00-2:00pm
Additional Topics and Closing
60 minutes

Introductions and Guidelines

01

Patrick Doyle
Jamie Blakley

unisys

Meet our team

Jamie Blakley
Law Enforcement SME

diverse COMPUTING

Mike Hulme
Lead Solution Architect

unisys

Terry Willert
Senior Technical
Delivery Manager

unisys

Patrick Doyle
Director, Justice & Law
Enforcement Practice

unisys

Keifer Hudson
DCI Technical Support

diverse COMPUTING

Jeff Corn
Architect

unisys

Virtual Team

Unisys

Jim Gschwend
Engagement Executive

Ravindra Kotikalapudi
Enterprise Architect

Kurt Martin
Cloud Architect

Theresa Huhn
LEMS Training Lead

Leighann Mansfield
Business Development Manager

Diverse Computing

Melissa Ehster
Product Development Manager

Nichole Moore
Chief Operating Officer

diverse COMPUTING

Product Approach and Overview

02

Patrick Doyle
Jamie Blakley

unisys

Why Unisys and DCI

Established, Attested

Unbeatable Pairing

Cloud Experts

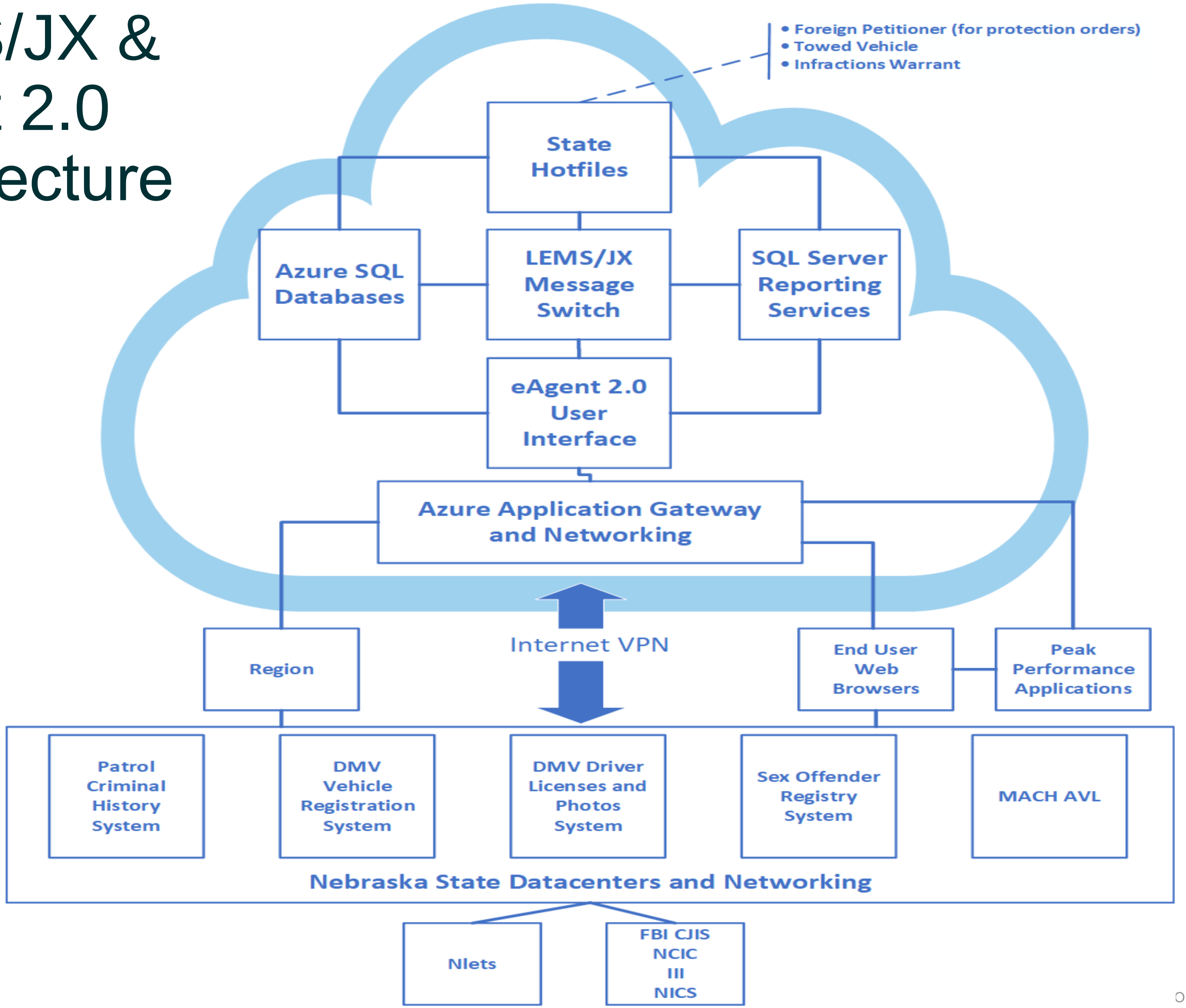
Customer Driven

Unisys LEMS/JX & DCI eAgent Product Overviews

- eAgent 2.0
- Zero Footprint End User Interface
- Customer Driven Design
- Flexible and Configurable
- Look for these Features
  - Hit Confirmation Workflow
  - eAgent Response Buttons (ERB)
  - VIN Assist
  - Smart Message
  - Device Independent
  - Team Inbox

- LEMS/JX -
- Highly attested/mature M/S tech stack
- Table driven with no code changes needed
- Complete & configurable message processing (parsing, field validations, reformatting, routing, etc.)
- Configurable interfaces using both modern and legacy technologies
- Cloud architected an eAgent 2.0 integrated
- Security supports both enterprise or application authentication
- Extremely reliable/2 billion+ messages routed yearly

Unisys LEMS/JX & DCI eAgent 2.0 "To Be" Architecture



- Foreign Petitioner (for protection orders)
- Towed Vehicle
- Infractions Warrant

State Hotfiles

Azure SQL Databases

LEMS/JX Message Switch

SQL Server Reporting Services

eAgent 2.0 User Interface

Azure Application Gateway and Networking

Internet VPN

Region

End User Web Browsers

Peak Performance Applications

Patrol Criminal History System

DMV Vehicle Registration System

DMV Driver Licenses and Photos System

Sex Offender Registry System

MACH AVL

Nebraska State Datacenters and Networking

Nlets

FBI CJIS
NCIC
III
NICS

Focused Demonstration Scenario 1

User maintenance

03

unisys

Scenario 1: User maintenance

Demonstrate / Present:

- □ user capabilities available to an agency and system administrator to create new users with various roles, and if applicable, how capabilities can be added or configured in the system
- □ process of adding each of the noted users with functions indicated above in Table 3
- □ process of updating the capabilities for three existing users in Table 3; for example, add a new capability to allow Community Service Officer Smith, created in step #2, above, to conduct record file maintenance and run reports and logs
- □ process of deactivating two of the above users
- □ how a user role can be removed for all users of an agency quickly without updating each and all users of that agency
- □ authentication process, including an overview of passwords and the sign-on process
- □ role-based user views once signed on to the system
- □ process for resetting a user password
- □ how a user would reset his/her own password

Scenario 1: User maintenance (continued)

Demonstrate / Present:

- □ process for adding and deactivating an MKE
- □ process for modifying an existing MKE
- □ process for making changes to message routing
- □ how to modify the originating agency identifier (ORI) table
- □ real-time system monitoring and diagnostics capabilities, including connectivity, central processing unit (CPU) utilization, and storage capacity
- □ ability to provide remote administrative access to the system
- □ ability to translate an ASCII dot delimited transaction to an XML schema and route that XML packet to a location using web services, then route the ASCII packet to another location
- □ ability to translate an XML schema received via web services to an ASCII dot delimited format and transmit that dot delimited transaction to a location
- □ ability to translate an XML schema received via web services to an ASCII dot delimited format, transmit that dot delimited transaction to a location, and transmit the XML packet to another location

Demonstrate/present the user capabilities available to an agency and system administrator to create new users with various roles

- NSP and local agency user administrators manage LEMS/JX / eAgent 2.0 user profiles using the LEMS/JX User Management Console
- NSP user administrators can manage all users
- Local agency user administrators can only manage users in their own agency
- NSP manages who is a local agency user administrator
- Permissions for eAgent 2.0 users and some local agency interface users are managed using LEMS/JX Function Groups
- Permissions for LEMS/JX Console users and LEMS/JX User Management Console users are managed using LEMS Console Roles

DEMO

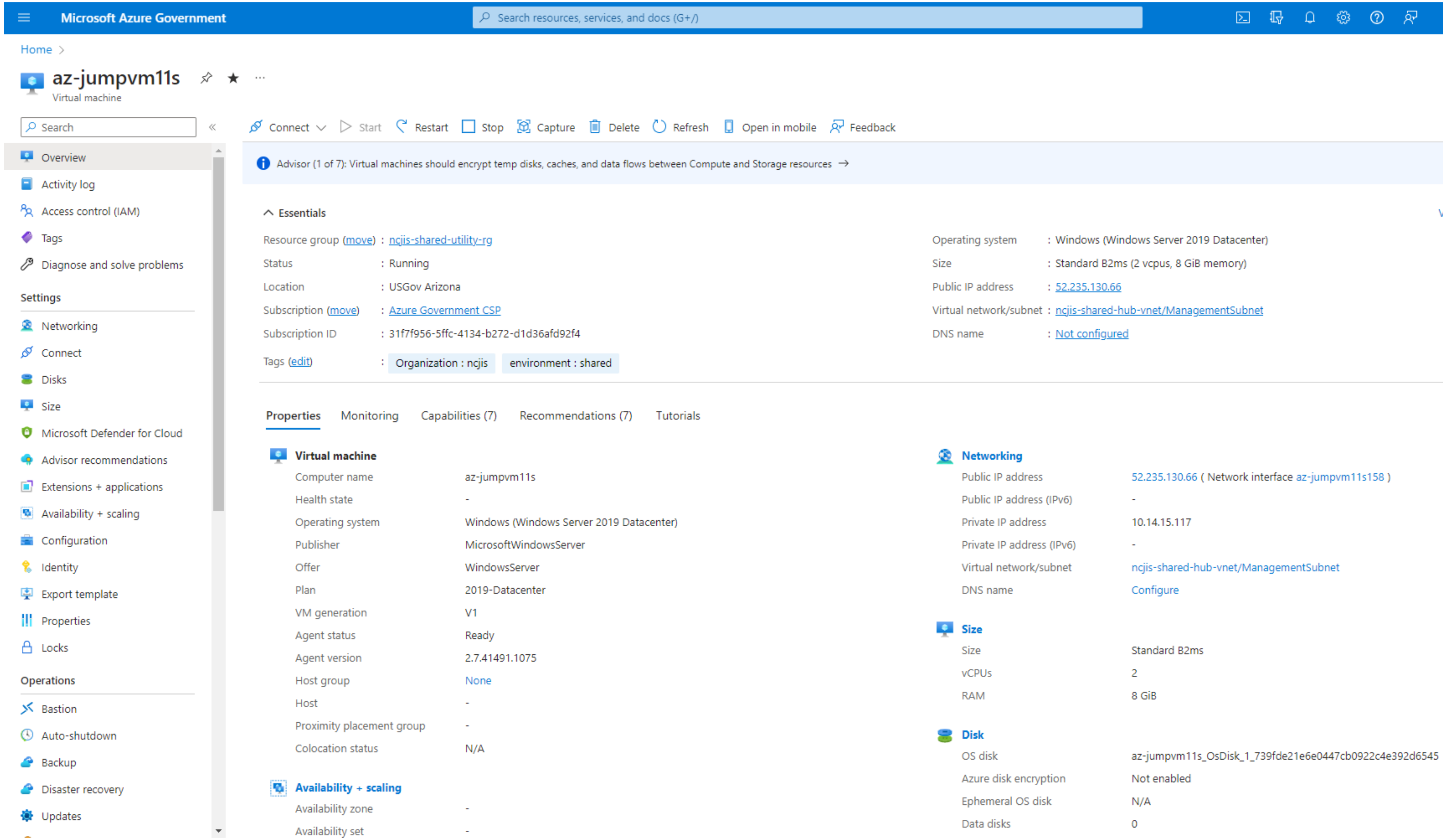
Authentication process, including an overview of passwords and the sign-on process

- Sign-on through eAgent 2.0 uses Azure Active Directory (AD) authentication – user ID, password, and multifactor authentication (MFA) – Authentication App (Microsoft, Google, FortiToken, YubiKey)
- If authentication is successful, eAgent 2.0 verifies user is enabled and certification not expired; retrieves function group
- Self-service Password Management application allows users to:
  - Set their email address for password expiration notifications
  - Change their password (to change their password before it expires)
  - Enroll in self-services password reset
  - Reset their password (to reset their password if they forgot it or it has expired)
- Video demonstration of Self-service Password Management

DEMO

SCENARIO 1

Real-time System Monitoring and Diagnostics Capabilities



az-jumpvm11s

Virtual machine

Advisor (1 of 7): Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources →

Essentials

Resource group (move)	: ncjis-shared-utility-rg	Operating system	: Windows (Windows Server 2019 Datacenter)
Status	: Running	Size	: Standard B2ms (2 vcpus, 8 GiB memory)
Location	: USGov Arizona	Public IP address	: 52.235.130.66
Subscription (move)	: Azure Government CSP	Virtual network/subnet	: ncjis-shared-hub-vnet/ManagementSubnet
Subscription ID	: 31f7f956-5ffc-4134-b272-d1d36afd92f4	DNS name	: Not configured
Tags (edit)	: Organization : ncjis environment : shared		

Virtual machine

Computer name	az-jumpvm11s
Health state	-
Operating system	Windows (Windows Server 2019 Datacenter)
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-Datacenter
VM generation	V1
Agent status	Ready
Agent version	2.7.41491.1075
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A

Availability + scaling

Availability zone	-
Availability set	-

Networking

Public IP address	52.235.130.66 (Network interface az-jumpvm11s158)
Public IP address (IPv6)	-
Private IP address	10.14.15.117
Private IP address (IPv6)	-
Virtual network/subnet	ncjis-shared-hub-vnet/ManagementSubnet
DNS name	Configure

Size

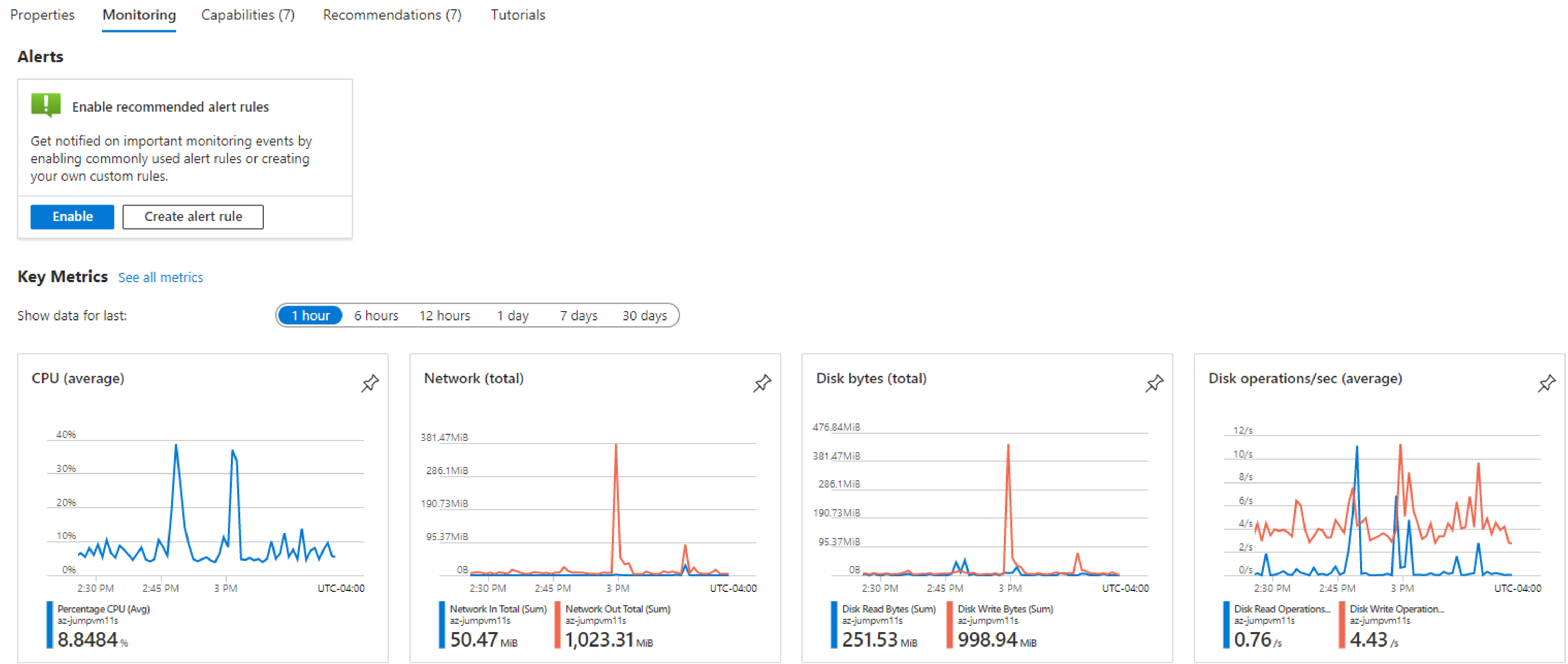
Size	Standard B2ms
vCPUs	2
RAM	8 GiB

Disk

OS disk	az-jumpvm11s_OsDisk_1_739fde21e6e0447cb0922c4e392d6545
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

diverse COMPUTING

Real-time System Monitoring and Diagnostics Capabilities



Alerts

Enable recommended alert rules

Get notified on important monitoring events by enabling commonly used alert rules or creating your own custom rules.

Key Metrics

See all metrics

Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

CPU (average)

Percentage CPU (Avg)
az-jumpvm11s
8.8484 %

Network (total)

Network In Total (Sum)
az-jumpvm11s
50.47 MiB

Network Out Total (Sum)
az-jumpvm11s
1,023.31 MiB

Disk bytes (total)

Disk Read Bytes (Sum)
az-jumpvm11s
251.53 MiB

Disk Write Bytes (Sum)
az-jumpvm11s
998.94 MiB

Disk operations/sec (average)

Disk Read Operations...
az-jumpvm11s
0.76 /s

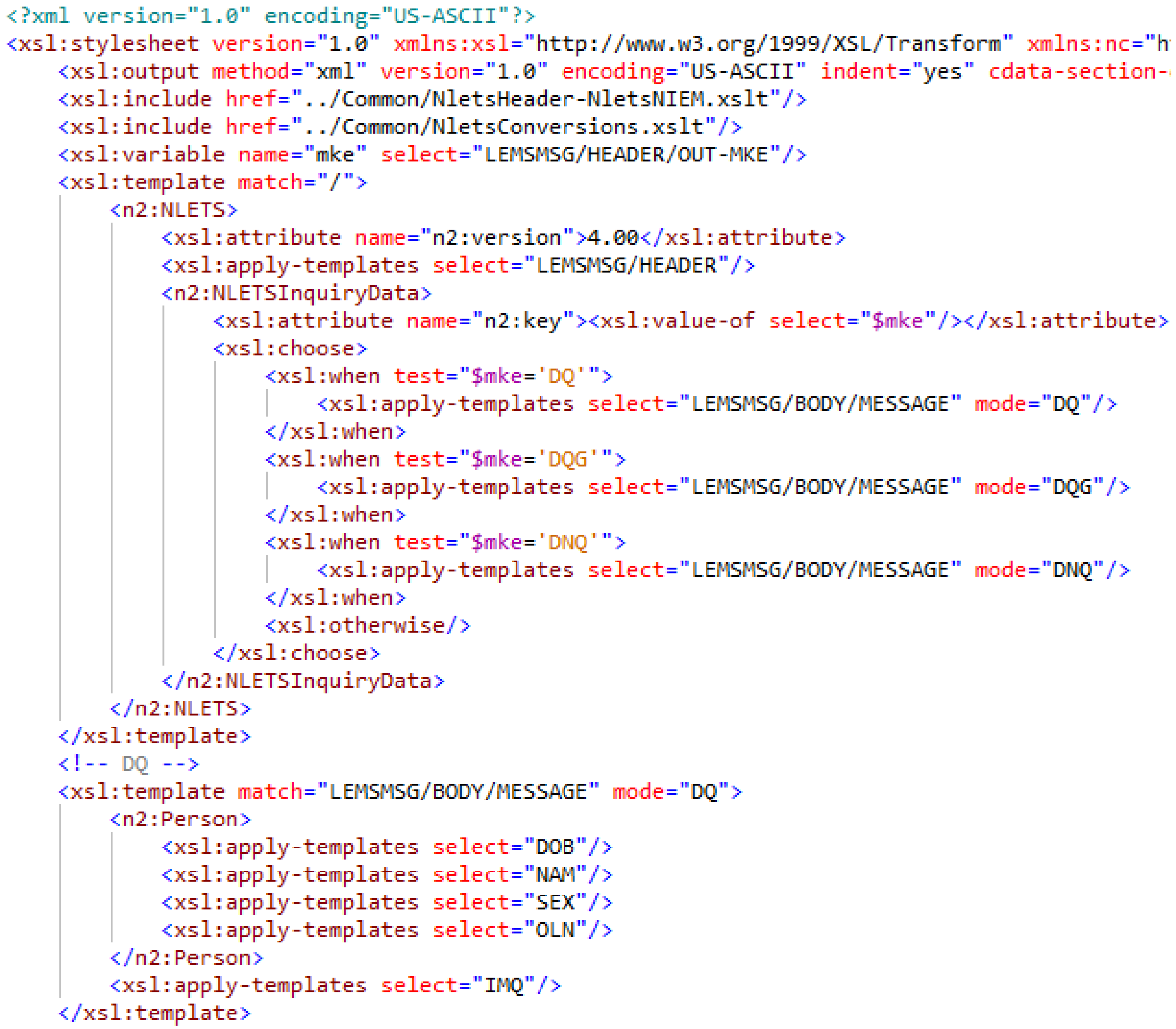
Disk Write Operation...
az-jumpvm11s
4.43 /s

Ability to provide remote administrative access to the system

- LEMS/JX User Management Console for administration of users and eAgent user inboxes/team inboxes
  - Agencies and NSP
- LEMS/JX Console for LEMS/JX operation, administration, and configuration (NSP)
- Microsoft Azure Government Portal for infrastructure administration

ASCII dot delimited and XML schema format transformation

- LEMS/JX uses XML Stylesheet Transformations (XSLT) to transform transactions from XML formats to other XML formats and to text
- XSLT is a W3C standard – not proprietary
- XSLT is defined in a stylesheet file written in XML and provides the transformation instructions
- XSLT files are tested, then deployed to production and take effect immediately without requiring any software code changes
- An “Output Stylesheet” specifies the transformation from an input transaction format to an output transaction format



```
<?xml version="1.0" encoding="US-ASCII"?>
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform" xmlns:nc="h
    <xsl:output method="xml" version="1.0" encoding="US-ASCII" indent="yes" cdata-section-
    <xsl:include href="../Common/NletsHeader-NletsNIEM.xslt"/>
    <xsl:include href="../Common/NletsConversions.xslt"/>
    <xsl:variable name="mke" select="LEMSMSG/HEADER/OUT-MKE"/>
    <xsl:template match="/">
        <n2:NLETS>
            <xsl:attribute name="n2:version">4.00</xsl:attribute>
            <xsl:apply-templates select="LEMSMSG/HEADER"/>
            <n2:NLETSInquiryData>
                <xsl:attribute name="n2:key"><xsl:value-of select="$mke"/></xsl:attribute>
                <xsl:choose>
                    <xsl:when test="$mke='DQ'">
                        <xsl:apply-templates select="LEMSMSG/BODY/MESSAGE" mode="DQ"/>
                    </xsl:when>
                    <xsl:when test="$mke='DQG'">
                        <xsl:apply-templates select="LEMSMSG/BODY/MESSAGE" mode="DQG"/>
                    </xsl:when>
                    <xsl:when test="$mke='DNQ'">
                        <xsl:apply-templates select="LEMSMSG/BODY/MESSAGE" mode="DNQ"/>
                    </xsl:when>
                    <xsl:otherwise/>
                </xsl:choose>
            </n2:NLETSInquiryData>
        </n2:NLETS>
    </xsl:template>
    <!-- DQ -->
    <xsl:template match="LEMSMSG/BODY/MESSAGE" mode="DQ">
        <n2:Person>
            <xsl:apply-templates select="DOB"/>
            <xsl:apply-templates select="NAM"/>
            <xsl:apply-templates select="SEX"/>
            <xsl:apply-templates select="OLN"/>
        </n2:Person>
        <xsl:apply-templates select="IMQ"/>
    </xsl:template>
```

Ability to translate an ASCII dot delimited transaction to an XML schema and route that XML packet to a location using web services, then route the ASCII packet to another location

- LEMS/JX provides a capability to automatically create an XML file in internal “LEMS Basic XML Format” from the fields parsed out of an ASCII dot delimited message
- A first output stylesheet is written and deployed to specify the transformation from the LEMS Basic XML Format to the output XML schema format
- A second output stylesheet is written and deployed to specify the transformation from the LEMS Basic XML Format to the output ASCII dot delimited format
- A first LEMS/JX output control entry specifies the first output stylesheet and destination for the web service
- A second LEMS/JX output control entry specifies the second output stylesheet and destination for other location

Ability to translate an XML schema received via web services to an ASCII dot delimited format and transmit that dot delimited transaction to a location

- An output stylesheet is written and deployed to specify the transformation from the web services XML Format to the output ASCII dot delimited format
- A LEMS/JX output control entry specifies the output stylesheet and destination for the location

Ability to translate an XML schema received via web services to an ASCII dot delimited format, transmit that dot delimited transaction to a location, and transmit the XML packet to another location

- A first output stylesheet is written and deployed to specify the transformation from the web services XML Format to the output ASCII dot delimited format
- A second output stylesheet is written and deployed to specify the transformation from the web services XML Format XML Format to the output XML schema format
- A first LEMS/JX output control entry specifies the first output stylesheet and destination for the other location
- A second LEMS/JX output control entry specifies the second output stylesheet and destination for web service

Scenario 1: User maintenance

Demonstrate / Present:

- ☑ user capabilities available to an agency and system administrator to create new users with various roles, and if applicable, how capabilities can be added or configured in the system
- ☑ process of adding each of the noted users with functions indicated above in Table 3
- ☑ process of updating the capabilities for three existing users in Table 3; for example, add a new capability to allow Community Service Officer Smith, created in step #2, above, to conduct record file maintenance and run reports and logs
- ☑ process of deactivating two of the above users
- ☑ how a user role can be removed for all users of an agency quickly without updating each and all users of that agency
- ☑ authentication process, including an overview of passwords and the sign-on process
- ☑ role-based user views once signed on to the system
- ☑ process for resetting a user password
- ☑ how a user would reset his/her own password

Scenario 1: User maintenance (continued)

Demonstrate / Present:

- ☑ process for adding and deactivating an MKE
- ☑ process for modifying an existing MKE
- ☑ process for making changes to message routing
- ☑ how to modify the originating agency identifier (ORI) table
- ☑ real-time system monitoring and diagnostics capabilities, including connectivity, central processing unit (CPU) utilization, and storage capacity
- ☑ ability to provide remote administrative access to the system
- ☑ ability to translate an ASCII dot delimited transaction to an XML schema and route that XML packet to a location using web services, then route the ASCII packet to another location
- ☑ ability to translate an XML schema received via web services to an ASCII dot delimited format and transmit that dot delimited transaction to a location
- ☑ ability to translate an XML schema received via web services to an ASCII dot delimited format, transmit that dot delimited transaction to a location, and transmit the XML packet to another location

Focused Demonstration Scenario 2

Reports and logging

03

unisys

Scenario 2: Reports and logging

Demonstrate / Present:

- □ range of available standard system logs
- □ utilization of user-based roles or permissions associated with the system logs
- □ process for generating a standard system log
- □ process for generating an ad hoc system log for audit purposes
- □ process of viewing, saving, and printing any system log that is generated
- □ how an administrator could generate both a daily log of system activity and an activity log for a specific user for a specific month
- □ utilization of user-based roles or permissions associated with the management reporting solution
- □ general management reporting solution proposed for the system
- □ range of available standard system management reports
- □ process for generating a standard management report

Scenario 2: Reports and logging

Demonstrate / Present:

□ generation and output of the following three sample reports:

- System uptime
- Number of transactions or inquiries performed by agency, for a user-definable period of time
- Number of input/output transactions conducted for a given period

□ process for generating an ad hoc report for data

□ how an administrator can select and export log data into CSV and XML formats

□ generation and output of the following three ad hoc reports:

- All transactions related to a specific vehicle, article, or person
- All transactions entered by a specific user
- All queries submitted by a specific user or agency

□ how an administrator could create a custom report of summary monthly administrative messaging by agency which will be generated quarterly

□ process of viewing, saving, printing, and deleting any report that is generated, including exports to other file formats, such as Excel, Word, or PDF

Scenario 2: Reports and logging

Logs & Ad-hoc Reporting Capabilities – Event Logs

Demonstrate / Present:

□ range of available standard system logs

□ process for generating a standard system log

□ process for generating an ad hoc system log for audit purposes

□ process of viewing, saving, and printing any system log that is generated

□ how an administrator could generate both a daily log of system activity and an activity log for a specific user for a specific month

□ process for generating an ad hoc report for data

Scenario 2: Reports and logging

Logs & Ad-hoc Reporting Capabilities – Event Logs – Cont.

Demonstrate / Present:

□ process for generating an ad hoc report for data

□ generation and output of the following three ad hoc reports:

- All transactions related to a specific vehicle, article, or person
- All queries submitted by a specific user or agency

□ how an administrator can select and export log data into CSV and XML formats

DEMO

Scenario 2: Reports and logging

Standard Management Reports – Overview

Demonstrate / Present:

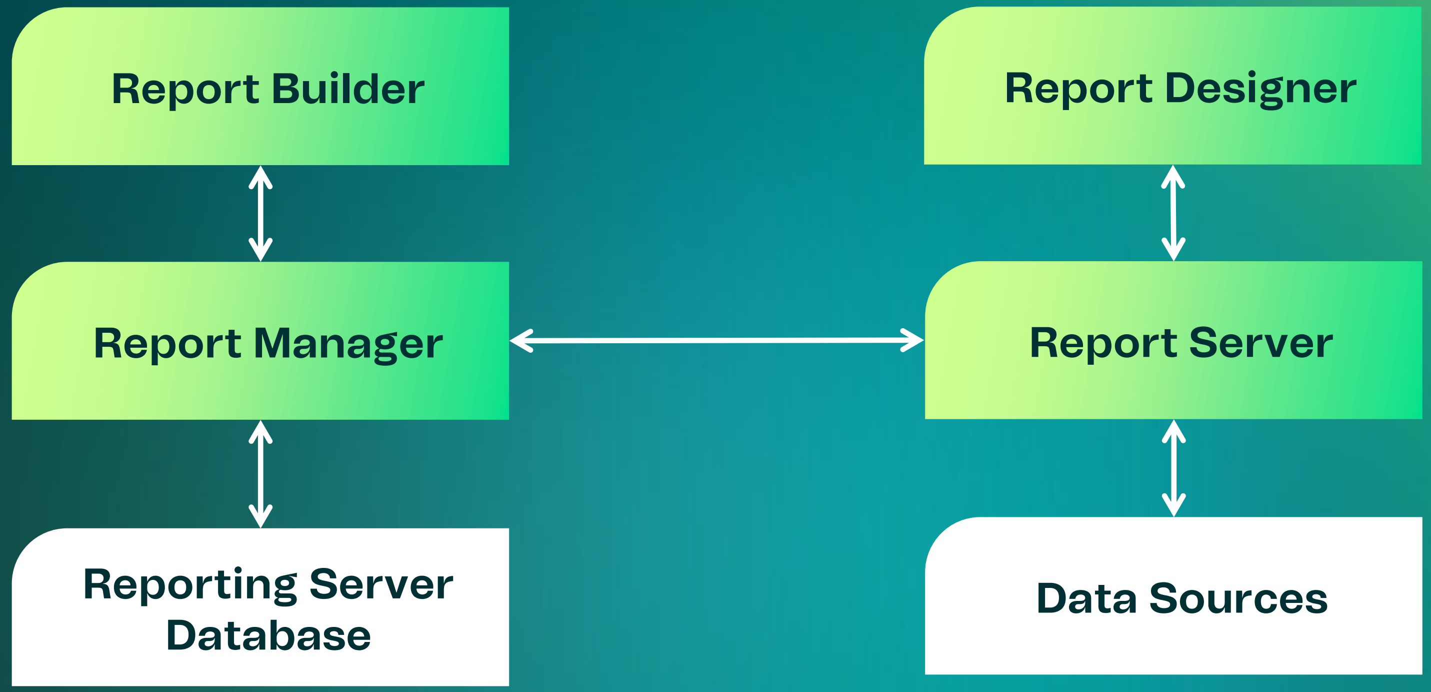
□ general management reporting solution proposed for the system

□ how an administrator could create a custom report of summary monthly administrative messaging by agency which will be generated quarterly

Scenario 2: Reports and logging

Standards Management Reports – Reporting Architecture

SSRS Architecture



Scenario 2: Reports and logging

Customized Reports – Report Builder

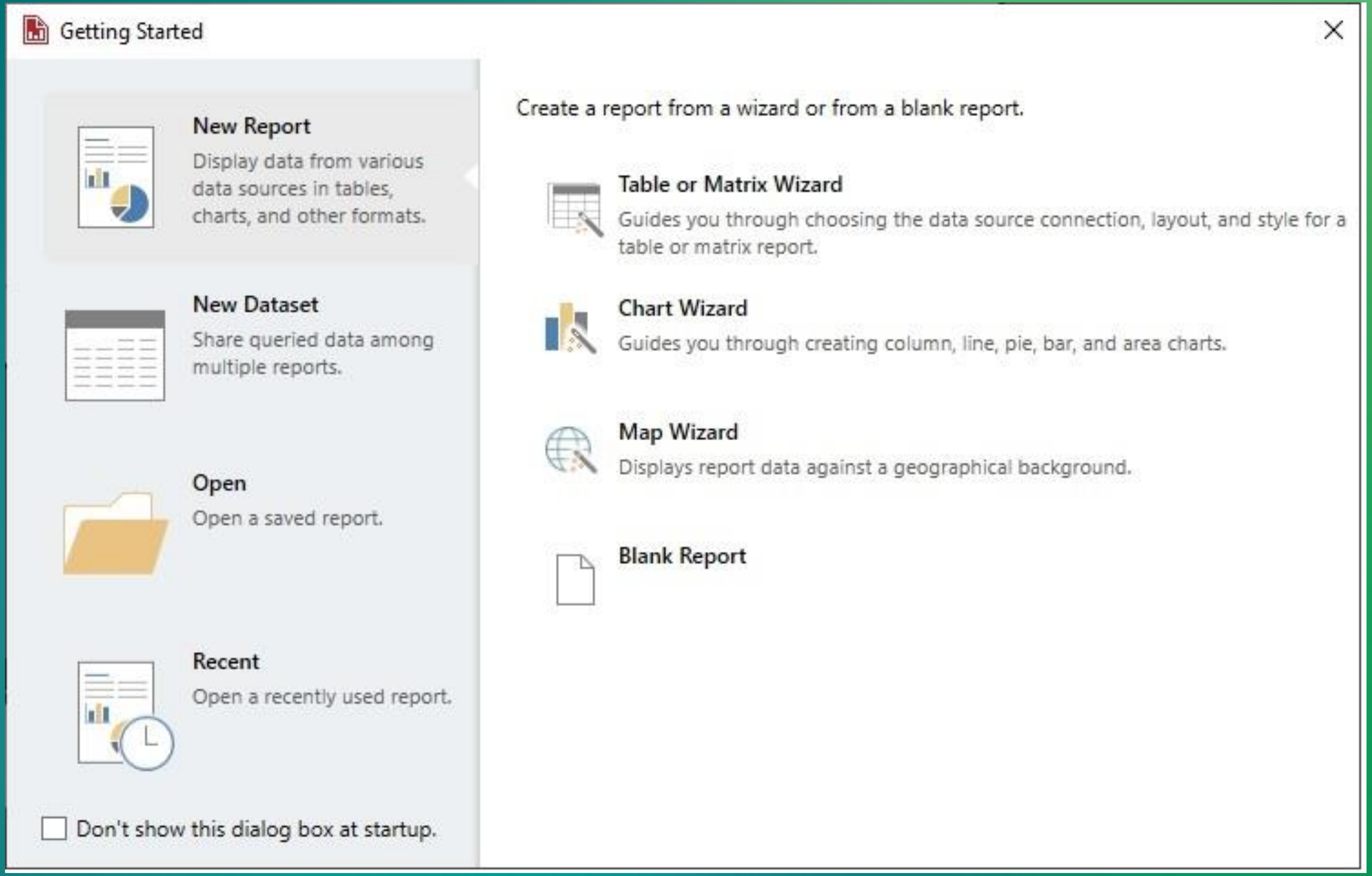
SQL Server – Report Builder

Guided Flow

Design Report Layout

Leveraged Shared Datasets

Targets: Power Users or IT Pros



Getting Started

New Report
Display data from various data sources in tables, charts, and other formats.

New Dataset
Share queried data among multiple reports.

Open
Open a saved report.

Recent
Open a recently used report.

□ Don't show this dialog box at startup.

Create a report from a wizard or from a blank report.

Table or Matrix Wizard
Guides you through choosing the data source connection, layout, and style for a table or matrix report.

Chart Wizard
Guides you through creating column, line, pie, bar, and area charts.

Map Wizard
Displays report data against a geographical background.

Blank Report

Scenario 2: Reports and logging

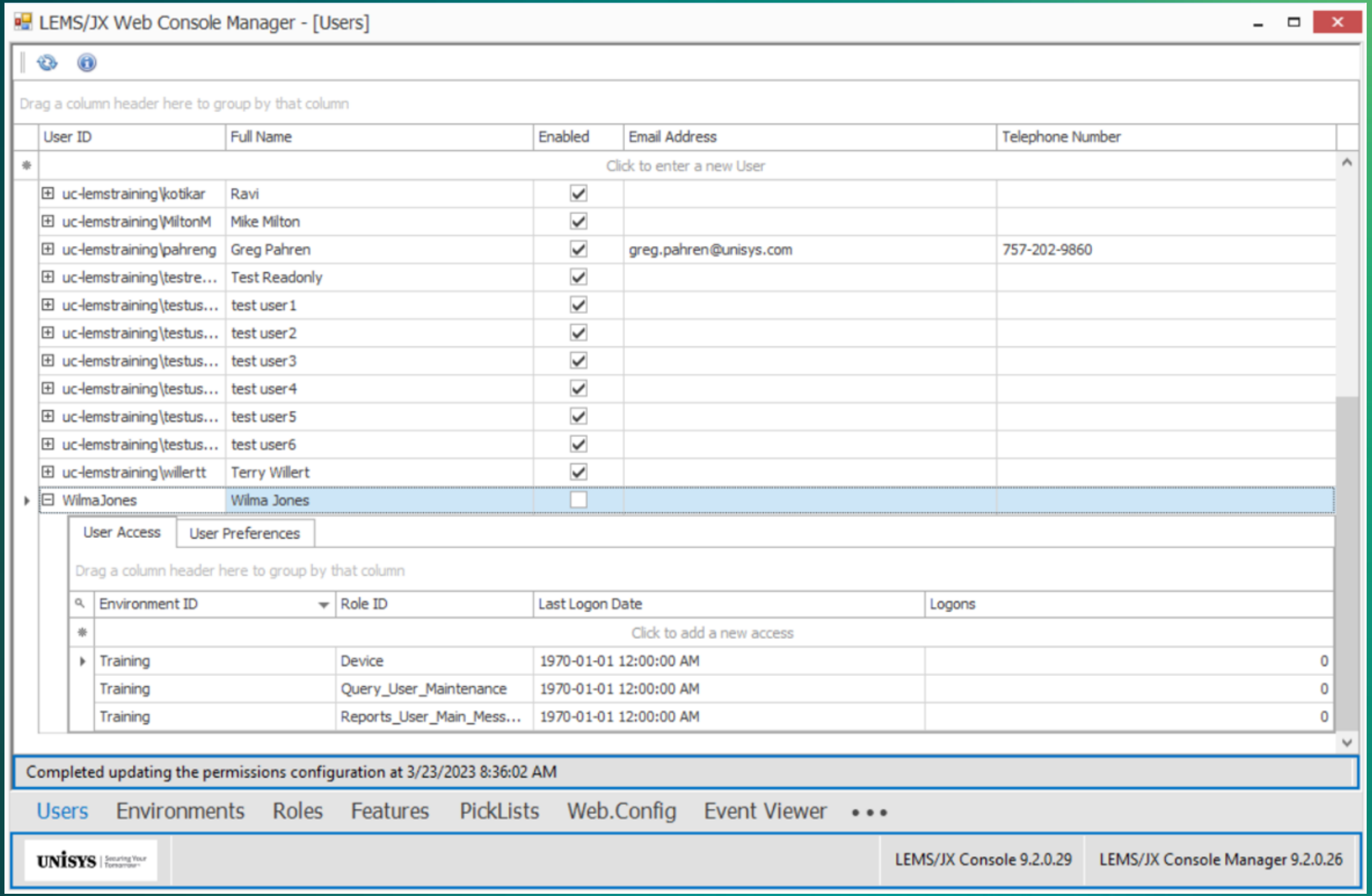
Standards Management Reports – Reporting Permission

Demonstrate / Present:

- □ utilization of user-based roles or permissions associated with the system logs
- □ utilization of user-based roles or permissions associated with the management reporting solution

Scenario 2: Reports and logging

Standard Management Reports – Reporting Permission – Cont.



LEMS/JX Web Console Manager - [Users]

Drag a column header here to group by that column

User ID	Full Name	Enabled	Email Address	Telephone Number
		Click to enter a new User		
⊞ uc-lemstraining\kotikar	Ravi	☑		
⊞ uc-lemstraining\MiltonM	Mike Milton	☑		
⊞ uc-lemstraining\pahreng	Greg Pahren	☑	greg.pahren@unisys.com	757-202-9860
⊞ uc-lemstraining\testre…	Test Readonly	☑		
⊞ uc-lemstraining\testus…	test user1	☑		
⊞ uc-lemstraining\testus…	test user2	☑		
⊞ uc-lemstraining\testus…	test user3	☑		
⊞ uc-lemstraining\testus…	test user4	☑		
⊞ uc-lemstraining\testus…	test user5	☑		
⊞ uc-lemstraining\testus…	test user6	☑		
⊞ uc-lemstraining\willertt	Terry Willert	☑		
⊟ WilmaJones	Wilma Jones	☐		

User Access | User Preferences

Drag a column header here to group by that column

Environment ID	Role ID	Last Logon Date	Logons
	Click to add a new access		
Training	Device	1970-01-01 12:00:00 AM	0
Training	Query_User_Maintenance	1970-01-01 12:00:00 AM	0
Training	Reports_User_Main_Mess…	1970-01-01 12:00:00 AM	0

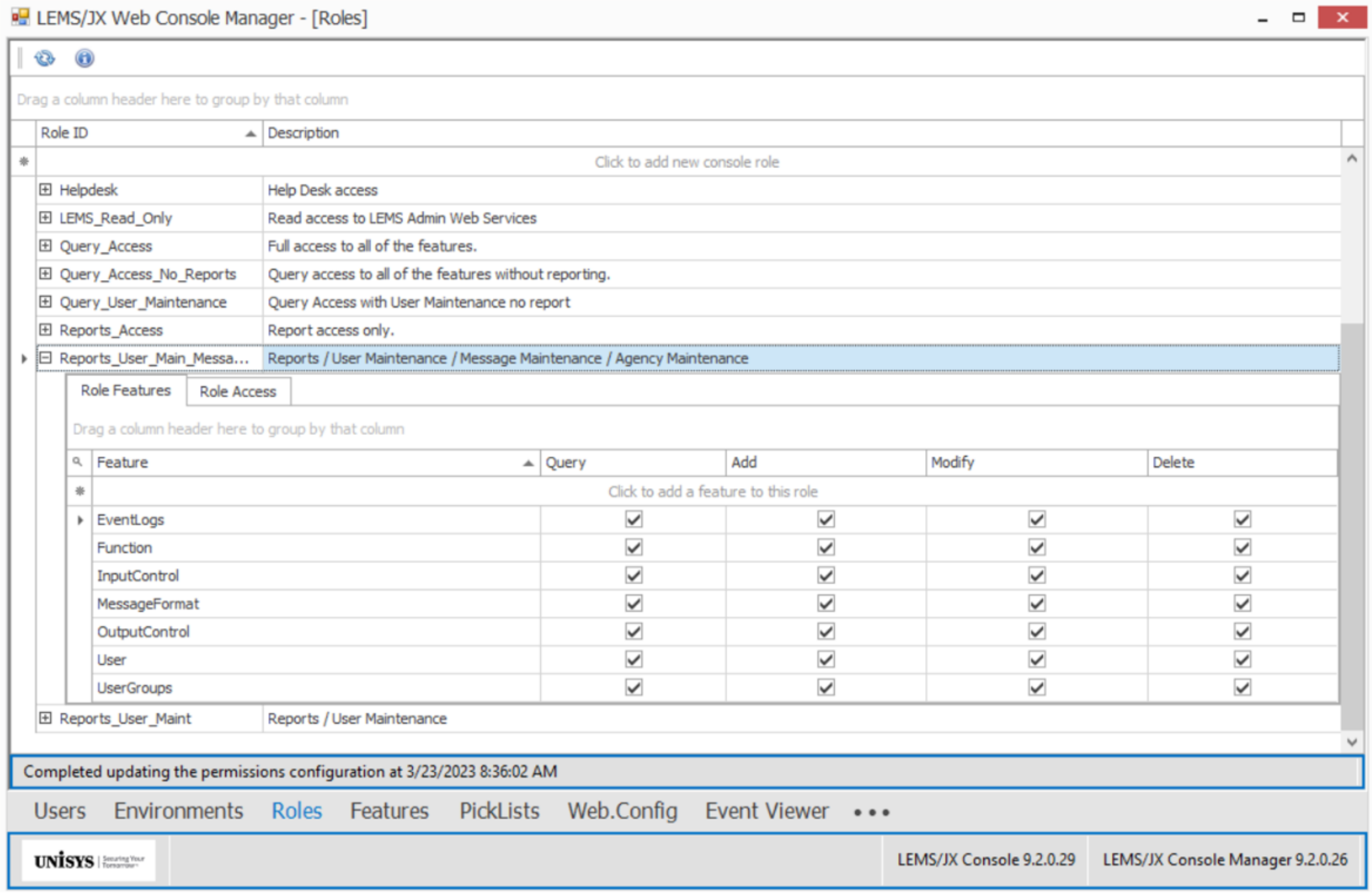
Completed updating the permissions configuration at 3/23/2023 8:36:02 AM

LEMS/JX Console 9.2.0.29

LEMS/JX Console Manager 9.2.0.26

Scenario 2: Reports and logging

Standard Management Reports – Reporting Permission – Cont.


LEMS/JX Web Console Manager - [Roles]
Drag a column header here to group by that column
Click to add new console role
Role Features
Role Access
Drag a column header here to group by that column
Click to add a feature to this role
Users
Environments
Roles
Features
PickLists
Web.Config
Event Viewer
• • •
UNISYS

Role ID	Description
⊞ Helpdesk	Help Desk access
⊞ LEMS_Read_Only	Read access to LEMS Admin Web Services
⊞ Query_Access	Full access to all of the features.
⊞ Query_Access_No_Reports	Query access to all of the features without reporting.
⊞ Query_User_Maintenance	Query Access with User Maintenance no report
⊞ Reports_Access	Report access only.
⊟ Reports_User_Main_Messa...	Reports / User Maintenance / Message Maintenance / Agency Maintenance
⊞ Reports_User_Maint	Reports / User Maintenance

Feature	Query	Add	Modify	Delete
EventLogs	☑	☑	☑	☑
Function	☑	☑	☑	☑
InputControl	☑	☑	☑	☑
MessageFormat	☑	☑	☑	☑
OutputControl	☑	☑	☑	☑
User	☑	☑	☑	☑
UserGroups	☑	☑	☑	☑

Completed updating the permissions configuration at 3/23/2023 8:36:02 AM

LEMS/JX Console 9.2.0.29   LEMS/JX Console Manager 9.2.0.26

Scenario 2: Reports and logging

Standards Management Reports – Statistics Report

Demonstrate / Present:

□ how an administrator could generate both a daily log of system activity and an activity log for a specific user for a specific month

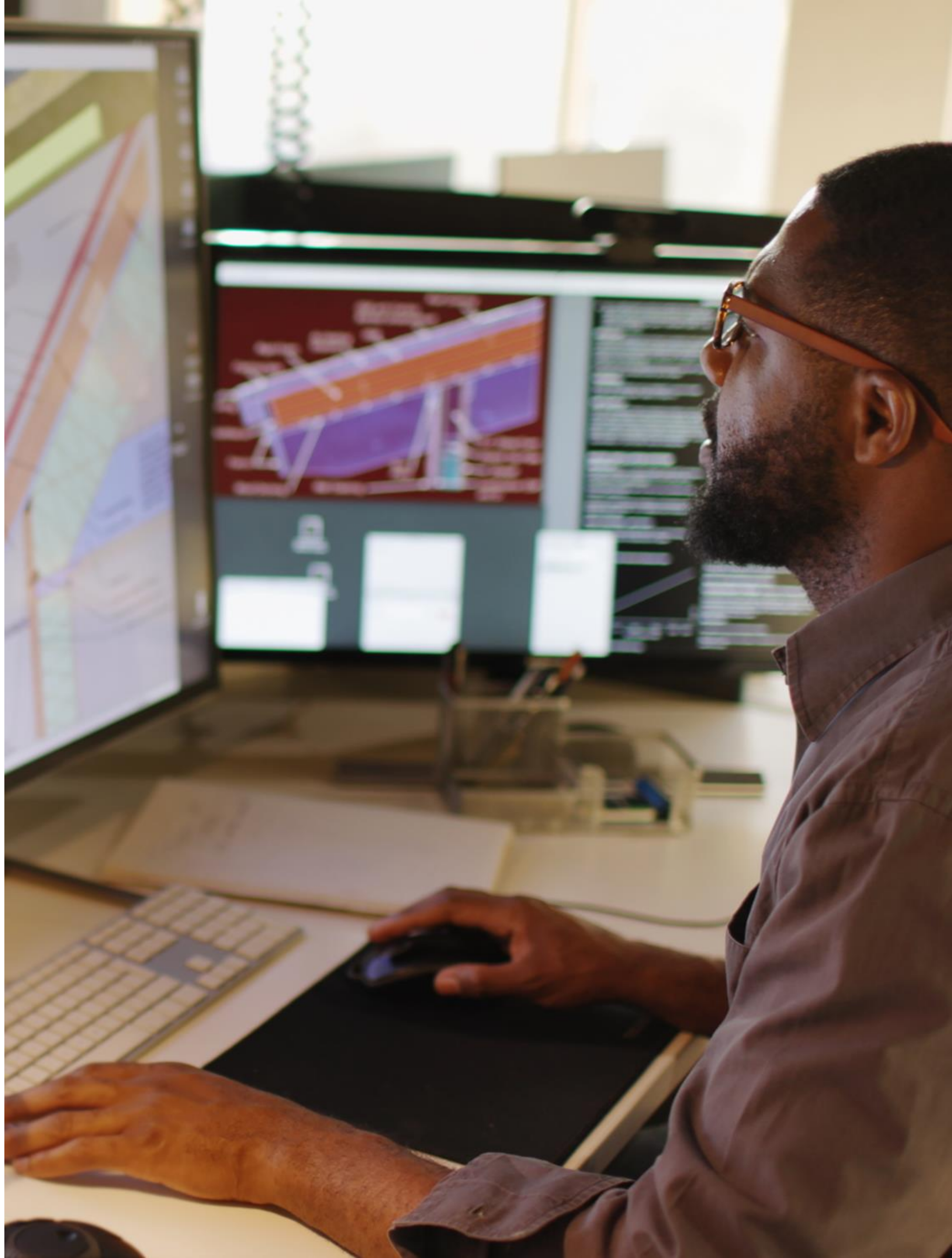
□ range of available standard system management reports

□ process for generating a standard management report

□ generation and output of the following three sample reports:

- Number of input/output transactions conducted for a given period

□ process of viewing, saving, printing, and deleting any report that is generated, including exports to other file formats, such as Excel, Word, or PDF

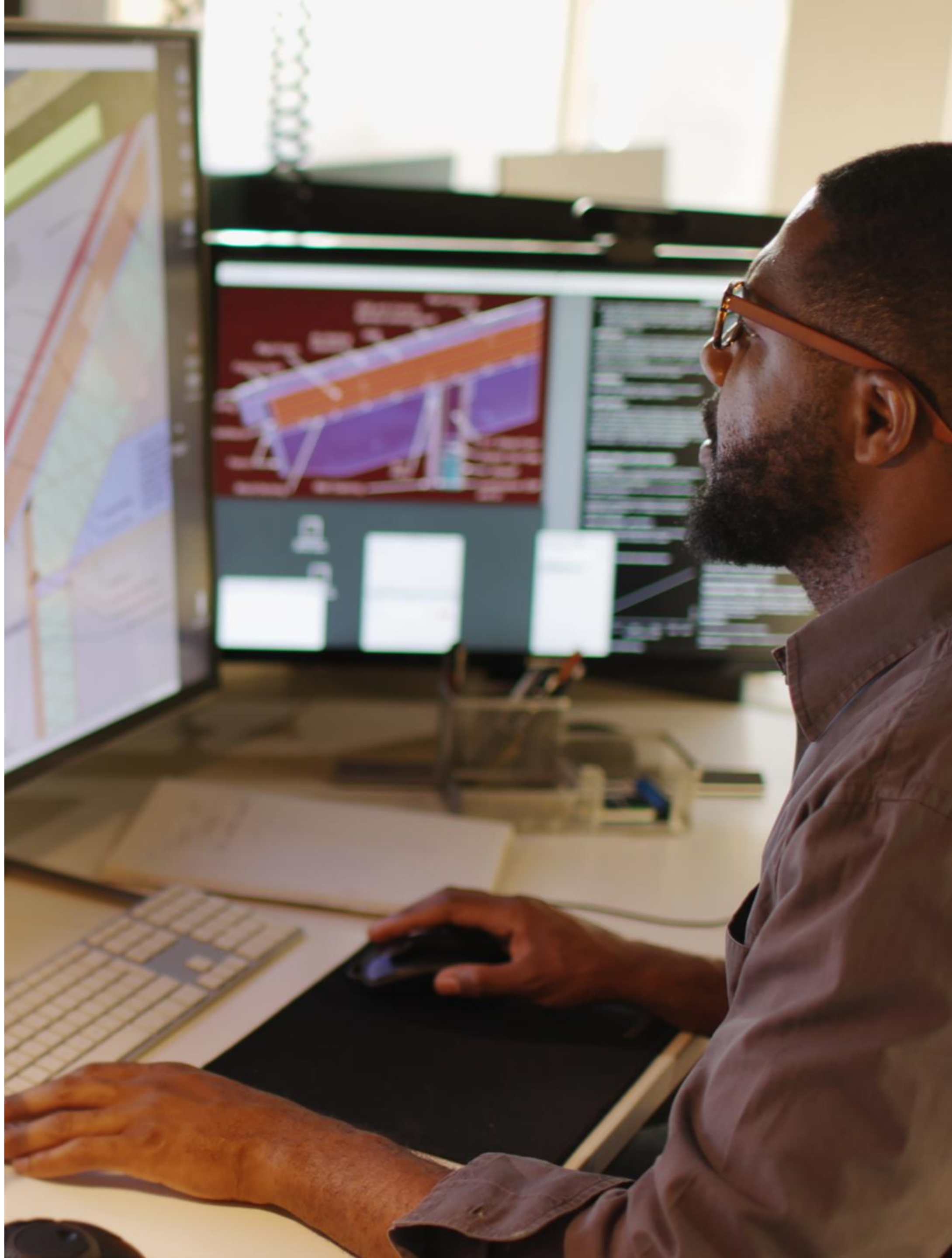


Scenario 2: Reports and logging

Standards Management Reports – Statistics Report – Cont.

Demonstrate / Present:

□ how an administrator can select and export log data into CSV and XML formats



DEMO

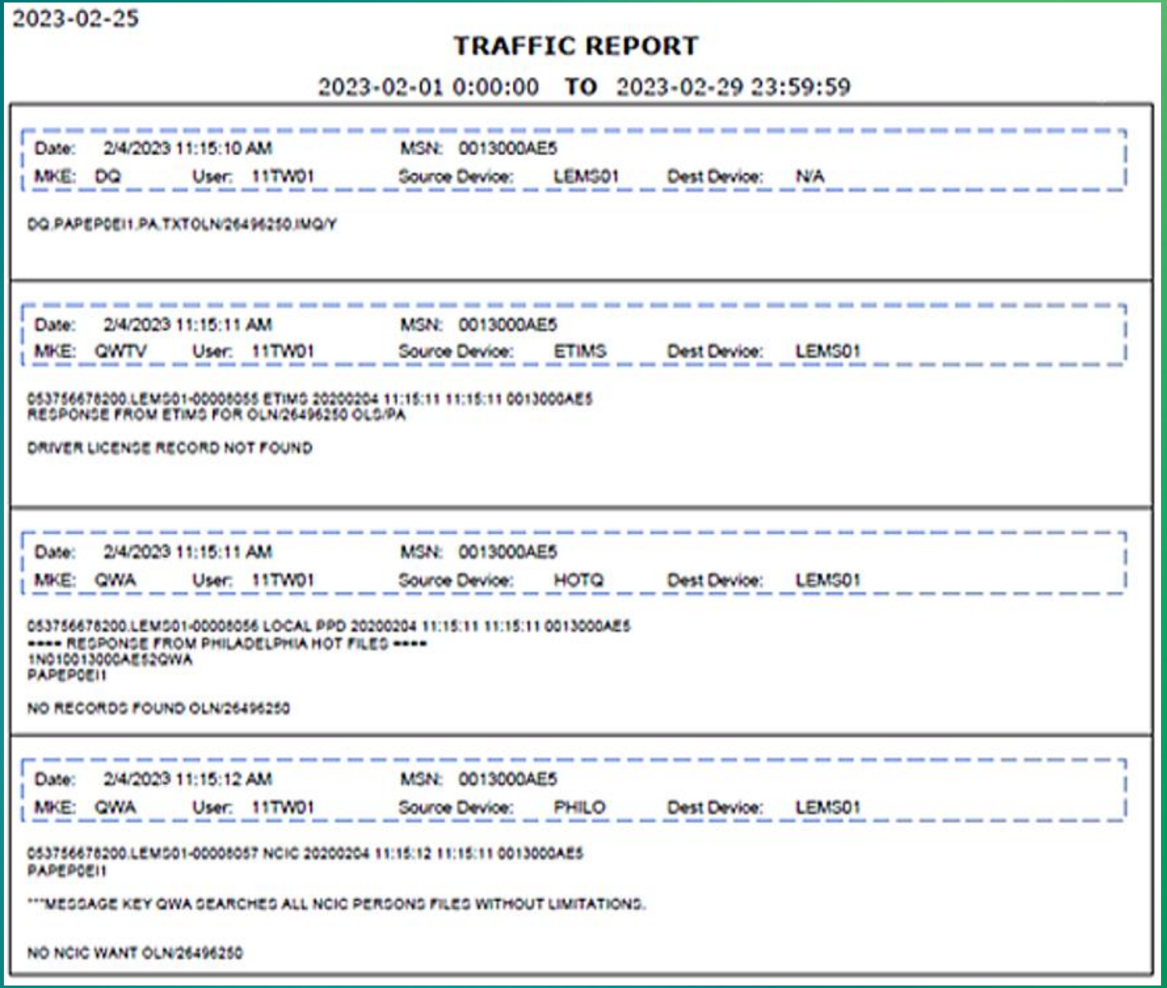
unisys

Scenario 2: Reports and logging

Daily activity for specific user

Demonstrate / Present:

- □ generation and output of the following three ad-hoc reports:
  - – All transactions entered by a specific user



```
2023-02-25
                          TRAFFIC REPORT
              2023-02-01 0:00:00   TO   2023-02-29 23:59:59

Date:   2/4/2023 11:15:10 AM              MSN:  0013000AE5
MKE:   DQ        User:  11TW01            Source Device:    LEMS01      Dest Device:    N/A

DQ.PAPEP0EI1.PA.TXTOLN/26496250.IMQ/Y

Date:   2/4/2023 11:15:11 AM              MSN:  0013000AE5
MKE:   QWTV      User:  11TW01            Source Device:    ETIMS       Dest Device:    LEMS01

053756678200.LEMS01-00008055 ETIMS 20200204 11:15:11 11:15:11 0013000AE5
RESPONSE FROM ETIMS FOR OLN/26496250 OLS/PA

DRIVER LICENSE RECORD NOT FOUND

Date:   2/4/2023 11:15:11 AM              MSN:  0013000AE5
MKE:   QWA       User:  11TW01            Source Device:    HOTQ        Dest Device:    LEMS01

053756678200.LEMS01-00008056 LOCAL PPD 20200204 11:15:11 11:15:11 0013000AE5
---- RESPONSE FROM PHILADELPHIA HOT FILES ----
1N01001300AE52QWA
PAPEP0EI1

NO RECORDS FOUND OLN/26496250

Date:   2/4/2023 11:15:12 AM              MSN:  0013000AE5
MKE:   QWA       User:  11TW01            Source Device:    PHILO       Dest Device:    LEMS01

053756678200.LEMS01-00008057 NCIC 20200204 11:15:12 11:15:11 0013000AE5
PAPEP0EI1

***MESSAGE KEY QWA SEARCHES ALL NCIC PERSONS FILES WITHOUT LIMITATIONS.

NO NCIC WANT OLN/26496250
```

unisys

diverse COMPUTING

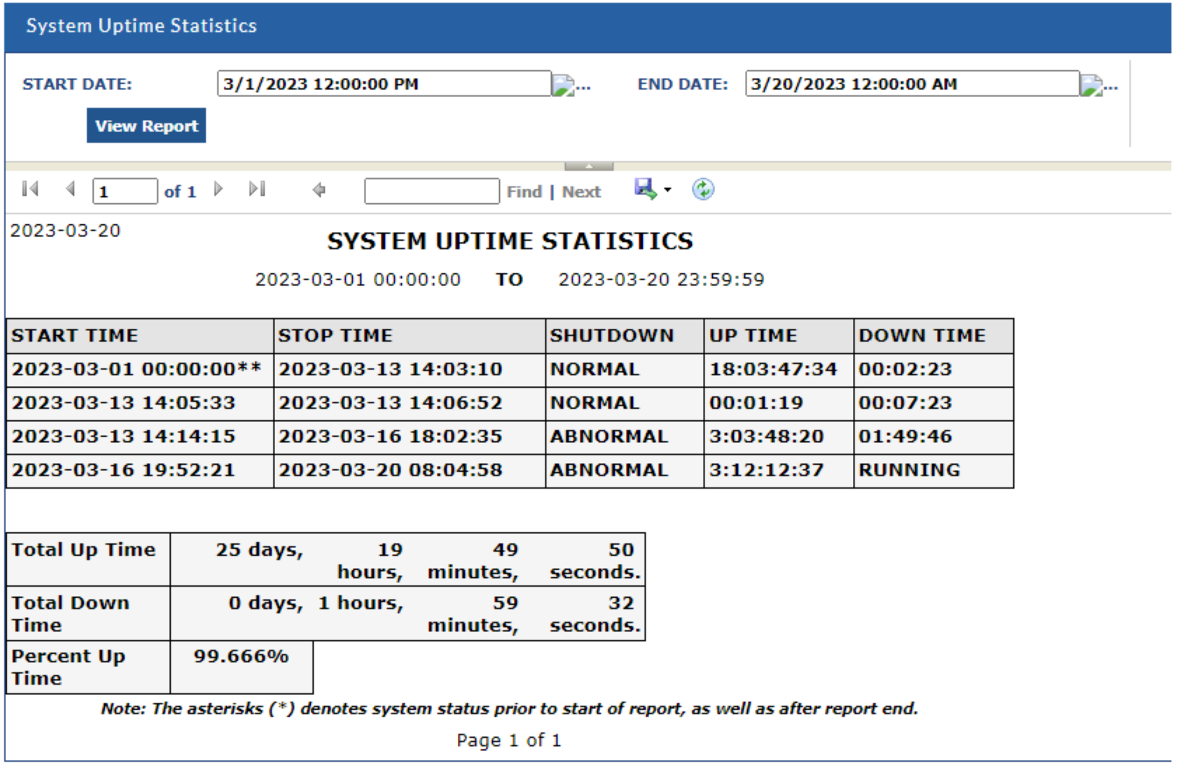
Scenario 2: Reports and logging

Uptime Report

Demonstrate / Present:

□ generation and output of the following three sample reports:

- System uptime



System Uptime Statistics

START DATE: 3/1/2023 12:00:00 PM

END DATE: 3/20/2023 12:00:00 AM

2023-03-20

SYSTEM UPTIME STATISTICS

2023-03-01 00:00:00 **TO** 2023-03-20 23:59:59

START TIME	STOP TIME	SHUTDOWN	UP TIME	DOWN TIME
2023-03-01 00:00:00**	2023-03-13 14:03:10	NORMAL	18:03:47:34	00:02:23
2023-03-13 14:05:33	2023-03-13 14:06:52	NORMAL	00:01:19	00:07:23
2023-03-13 14:14:15	2023-03-16 18:02:35	ABNORMAL	3:03:48:20	01:49:46
2023-03-16 19:52:21	2023-03-20 08:04:58	ABNORMAL	3:12:12:37	RUNNING

Total Up Time	25 days,	19 hours,	49 minutes,	50 seconds.
Total Down Time	0 days,	1 hours,	59 minutes,	32 seconds.
Percent Up Time	99.666%			

Note: The asterisks (*) denotes system status prior to start of report, as well as after report end.

Page 1 of 1

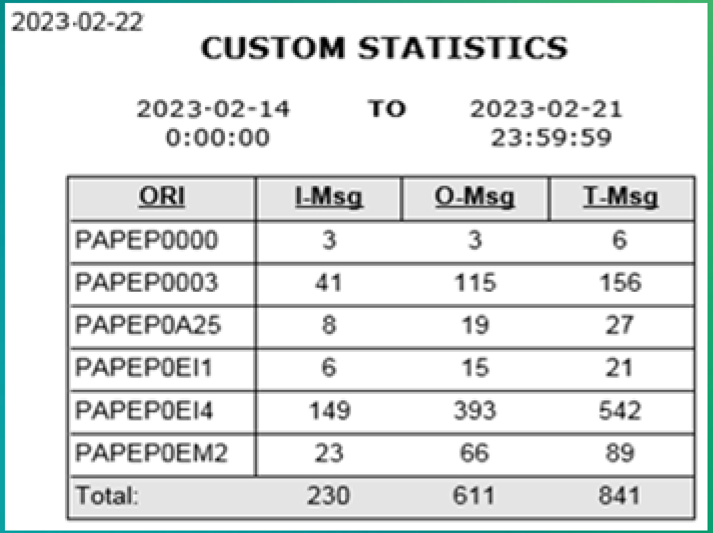
Scenario 2: Reports and logging

Custom Statistics by Agency

Demonstrate / Present:

□ following three sample reports:

- Number of transactions or inquiries performed by agency, for a user-definable period of time



2023-02-22

CUSTOM STATISTICS

2023-02-14 0:00:00 TO 2023-02-21 23:59:59

ORI	I-Msg	O-Msg	T-Msg
PAPEP0000	3	3	6
PAPEP0003	41	115	156
PAPEP0A25	8	19	27
PAPEP0EI1	6	15	21
PAPEP0EI4	149	393	542
PAPEP0EM2	23	66	89
Total:	230	611	841

Scenario 2: Reports and logging

Demonstrate / Present:

- ☑ range of available standard system logs
- ☑ utilization of user-based roles or permissions associated with the system logs
- ☑ process for generating a standard system log
- ☑ process for generating an ad hoc system log for audit purposes
- ☑ process of viewing, saving, and printing any system log that is generated
- ☑ how an administrator could generate both a daily log of system activity and an activity log for a specific user for a specific month
- ☑ utilization of user-based roles or permissions associated with the management reporting solution
- ☑ general management reporting solution proposed for the system
- ☑ range of available standard system management reports
- ☑ process for generating a standard management report

Scenario 2: Reports and logging

Demonstrate / Present:

☑ generation and output of the following three sample reports:

- System uptime
- Number of transactions or inquiries performed by agency, for a user-definable period of time
- Number of input/output transactions conducted for a given period

☑ process for generating an ad hoc report for data

☑ how an administrator can select and export log data into CSV and XML formats

☑ generation and output of the following three ad hoc reports:

- All transactions related to a specific vehicle, article, or person
- All transactions entered by a specific user
- All queries submitted by a specific user or agency

☑ how an administrator could create a custom report of summary monthly administrative messaging by agency which will be generated quarterly

☑ process of viewing, saving, printing, and deleting any report that is generated, including exports to other file formats, such as Excel, Word, or PDF

Break

04

Focused Demonstration Scenario 3

MSS Interfaces

05

Scenario 3: MSS Interfaces

Demonstrate / Present:

□ logging into the user interface

□ how the graphical user interface (GUI) utilizes features such as drop-down menus, autofill, and lookup tables

□ processing of responses back from NCIC such as the capture and forwarding of "$" messages through the proposed message switch

□ process of viewing, saving, printing, and deleting the system responses received from a wanted person entry as well as other solicited messages

□ how the system performs image processing

□ batch file processing

□ following record queries:

- Query vehicle (QV)
- Driver query (DQ)
- Criminal history search (QH)

□ sending of an administrative message to a group of agencies

□ process of viewing, saving, printing, and deleting administrative messages received as well as other unsolicited messages

□ Discuss options for providing statewide training user interface

□ Understanding of existing external interface protocols

□ following interfaces:

- DMV interface
- Web service to Nlets
- Web service from an in-state agency to NSP

□ product readiness for XML interfaces

DEMO

unisys

Batch File Processing

- The LEMS/JX batch file capability provides the ability to read transaction requests from input batch files and write responses to output batch files
- Input batch files are transferred by external systems or administrators to batch folders accessible by LEMS/JX
- Output batch files are transferred by external systems or administrators from the batch folders accessible by LEMS/JX
- Batch LEMS/JX devices are used to read the input batch files and write the output batch files
- Two methods are available:
  - Run whenever an input batch file appears in a specified folder
  - Run specified input batch file on specified days of the week and times
- Note that FBI CJIS does not support batch queries (QAB, QBB, QGB, QSB, QVB, QWB) in NCIC NIEM XML

Understanding of existing external interface protocols

- National systems: Unisys is an industry leader in the implementation of modern national interface standards – the first or among the first few
  - Nlets NIEM web services
  - NCIC NIEM web services
  - III NIEM web services
  - NICS NIEM web services
- State systems: Unisys applies our system integration expertise and LEMS/JX interface capabilities to configure legacy interface technologies (e.g., TCP/IP socket, IBM mainframe) and modern interface technologies (e.g., XML web services) required for state systems
  - Patrol Criminal History (PCH)
  - DMV vehicle registrations, driver licenses, and photos
  - Sex offender registry
  - MACH AVL

- Local agency systems:
  - Modern: LEMS Web Services: standards-based NIEM XML web services
  - Legacy: DMPP-2020/OFML

Specific interfaces

- DMV interface
  - Vehicle Title and Registration: LEMS/JX web services interface configured to conform to existing specifications provided by DMV/NSP
  - Driver licenses and photos: IBM mainframe interface using Microsoft Host Integration Server or other interface specifications provided by DMV/NSP
- Web service to Nlets
  - Standard Nlets NIEM web services – all Nlets transactions (in production in other states)
- Web service from an in-state agency to NSP (in production in other states)
  - LEMS Request Service provided by LEMS/JX and consumed by in-state agency to send request messages
  - LEMS Response Service provided by in-state agency and consumed by LEMS/JX to receive response messages and unsolicited messages
  - Simple, Web Services-Interoperability (WS-I) compliant Soap web service
  - Uses standard Nlets, NCIC, III, NICS, and State XML formats – no reinventing the wheel with a proprietary XML format
  - Uses Transport Layer Security (TLS) with certificate-based mutual authentication and FIPS 140-2 certified cryptographic modules for CJISSECPOL compliant encryption and authentication

SCENARIO 3

Product readiness for XML interfaces

- Unisys has provided XML capabilities in LEMS/JX for over 20 years and is an industry leader in the implementation of XML interfaces
- LEMS/JX provides highly configurable capabilities for XML interfaces and XML message handling
  - Parsing XML input messages using parsing stylesheet files
  - Validating parsed XML input message field content and relationships using LEMS/JX validation tables
  - Transforming from dot-slash or any parsable input message format to XML output format using stylesheet files
  - Transforming an XML input message format to a different output XML format using stylesheet files
  - Transforming an XML input message format to a text or output XML format using stylesheet files
  - Specification of parsing stylesheet files in input control table
  - Specification of output stylesheet files in output control table
  - XML Groups to specify interfaces that use the same XML formats

Statewide Training

□ Discuss options for providing statewide training user interface

- Statewide Train the Trainer
- Training system with simulated responses

Scenario 3: MSS Interfaces

Demonstrate / Present:

☑ logging into the user interface

☑ how the graphical user interface (GUI) utilizes features such as drop-down menus, autofill, and lookup tables

☑ processing of responses back from NCIC such as the capture and forwarding of "$" messages through the proposed message switch

☑ process of viewing, saving, printing, and deleting the system responses received from a wanted person entry as well as other solicited messages

☑ how the system performs image processing

☑ batch file processing

☑ following record queries:

- Query vehicle (QV)
- Driver query (DQ)
- Criminal history search (QH)

☑ sending of an administrative message to a group of agencies

☑ process of viewing, saving, printing, and deleting administrative messages received as well as other unsolicited messages

☑ Discuss options for providing statewide training user interface

☑ Understanding of existing external interface protocols

☑ following interfaces:

- DMV interface
- Web service to Nlets
- Web service from an in-state agency to NSP

☑ product readiness for XML interfaces

Focused Demonstration Scenario 4

Administrative maintenance

05

unisys

Scenario 4: Administrative maintenance

Demonstrate / Present:

□ process of performing a system shutdown and restart under routine and emergency situations

□ any tools or GUIs that would be used to monitor the real-time status of the MSS

□ any tools or GUIs that would be used to monitor/verify the status of interface (NCIC, Nlets, DMV, etc.) connections

□ process of creating, modifying, and maintaining product forms and how those forms are rolled out to the clients

□ process of adding and disabling various codes (ORIs, uniform offense codes, vehicle codes, etc.) to the MSS code database/tables

Scenario 4: Administrative maintenance

Demonstrate / Present:

□ process of performing a system shutdown and restart under routine and emergency situations

□ any tools or GUIs that would be used to monitor the real-time status of the MSS

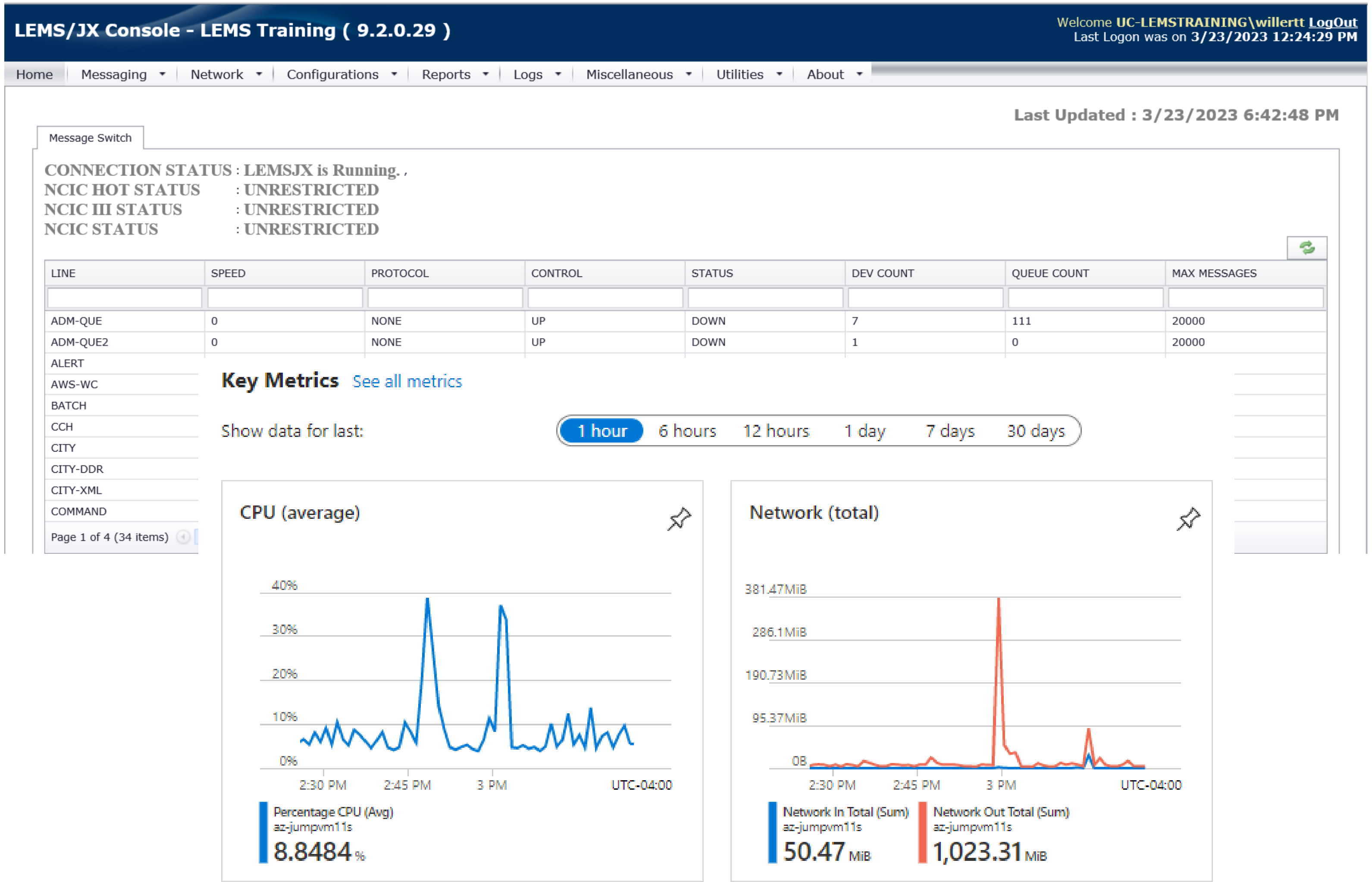
□ any tools or GUIs that would be used to monitor/verify the status of interface (NCIC, Nlets, DMV, etc.) connections

Performing a system shutdown and restart under routine and emergency situations

- LEMS/JX is manually shut down, restarted, and failed over to the secondary virtual machine using Microsoft Failover Cluster Manager for both routine and emergency situations
- Microsoft Failover Cluster automatically transfers LEMS/JX operation from the primary VM to the secondary VM in the rare event the primary VM fails

Tools or GUIs that would be used to monitor the real-time status of the MSS

- The LEMS/JX Console is used to monitor the real-time status of the LEMS/JX application
- The Azure Government Portal is used to monitor the real-time status of the MSS infrastructure
- Azure Application Monitoring is configured to notify support personnel of
  - Infrastructure failure events
  - Key LEMS/JX interface status changes (up to down)
  - Other key LEMS/JX events requiring operational support, such as queues exceeding a specified threshold


LEMS/JX Console - LEMS Training (9.2.0.29)
Welcome UC-LEMSTRAINING\willertt LogOut
Last Logon was on 3/23/2023 12:24:29 PM
Home
Messaging
Network
Configurations
Reports
Logs
Miscellaneous
Utilities
About
Message Switch

Last Updated : 3/23/2023 6:42:48 PM

CONNECTION STATUS : LEMSJX is Running. ,
NCIC HOT STATUS : UNRESTRICTED
NCIC III STATUS : UNRESTRICTED
NCIC STATUS : UNRESTRICTED

LINE	SPEED	PROTOCOL	CONTROL	STATUS	DEV COUNT	QUEUE COUNT	MAX MESSAGES
ADM-QUE	0	NONE	UP	DOWN	7	111	20000
ADM-QUE2	0	NONE	UP	DOWN	1	0	20000
ALERT							
AWS-WC							
BATCH							
CCH							
CITY							
CITY-DDR							
CITY-XML							
COMMAND							

Page 1 of 4 (34 items)

Key Metrics See all metrics

Show data for last: [✓ 1 hour] 6 hours 12 hours 1 day 7 days 30 days

Tools or GUIs that would be used to monitor/verify the status of interface (NCIC, Nlets, DMV, etc.) connections

- The LEMS/JX Console is used to monitor the real-time status of the LEMS/JX interfaces
- Azure Application Monitoring is configured to notify support personnel of
  - LEMS/JX interface status changes
  - LEMS/JX interface queues exceeding a specified threshold

Scenario 4: Administrative maintenance

Demonstrate / Present:

□ process of creating, modifying, and maintaining product forms

and how those forms are rolled out to the clients

Scenario 4: Administrative maintenance

Demonstrate / Present:

□ process of adding and disabling various codes (ORIs, uniform offense codes, vehicle codes, etc.) to the MSS code database/tables

DEMO

Scenario 4: Administrative maintenance

Demonstrate / Present:

- ☑ process of performing a system shutdown and restart under routine and emergency situations
- ☑ any tools or GUIs that would be used to monitor the real-time status of the MSS
- ☑ any tools or GUIs that would be used to monitor/verify the status of interface (NCIC, Nlets, DMV, etc.) connections
- ☑ process of creating, modifying, and maintaining product forms and how those forms are rolled out to the clients
- ☑ process of adding and disabling various codes (ORIs, uniform offense codes, vehicle codes, etc.) to the MSS code database/tables

Focused Demonstration Scenario 5

Hot Files

05

Scenario 5: Hot Files

Demonstrate / Present:

□ general hot file maintenance solution proposed for the system

□ entry of a general wanted person record into the system, both via a command line and the GUI

□ processing of a wanted person entry into NCIC, and include a demonstration of how the wanted person entry generates specific types of messages through the system

□ ability to run a report of hot files data (e.g., the number of open warrants from a specific ORI or statewide)

□ utilization of user-based roles or permissions associated with the hot file maintenance solution

□ following hot file record queries:

Query wanted person (QW)

Registration query (RQ)

Query all state warrants (QWA)

□ processing of a towed vehicle entry into Nebraska's hot file system

□ processing of a wanted person into Nebraska's hot file system

Scenario 5: Hot Files

Demonstrate / Present:

□ general hot file maintenance solution proposed for the system

□ entry of a general wanted person record into the system, both via a command line and the GUI

□ processing of a wanted person entry into NCIC, and include a demonstration of how the wanted person entry generates specific types of messages through the system

□ utilization of user-based roles or permissions associated with the hot file maintenance solution

□ following hot file record queries:

Query wanted person (QW)

Registration query (RQ)

Query all state warrants (QWA)

□ processing of a towed vehicle entry into Nebraska's hot file system

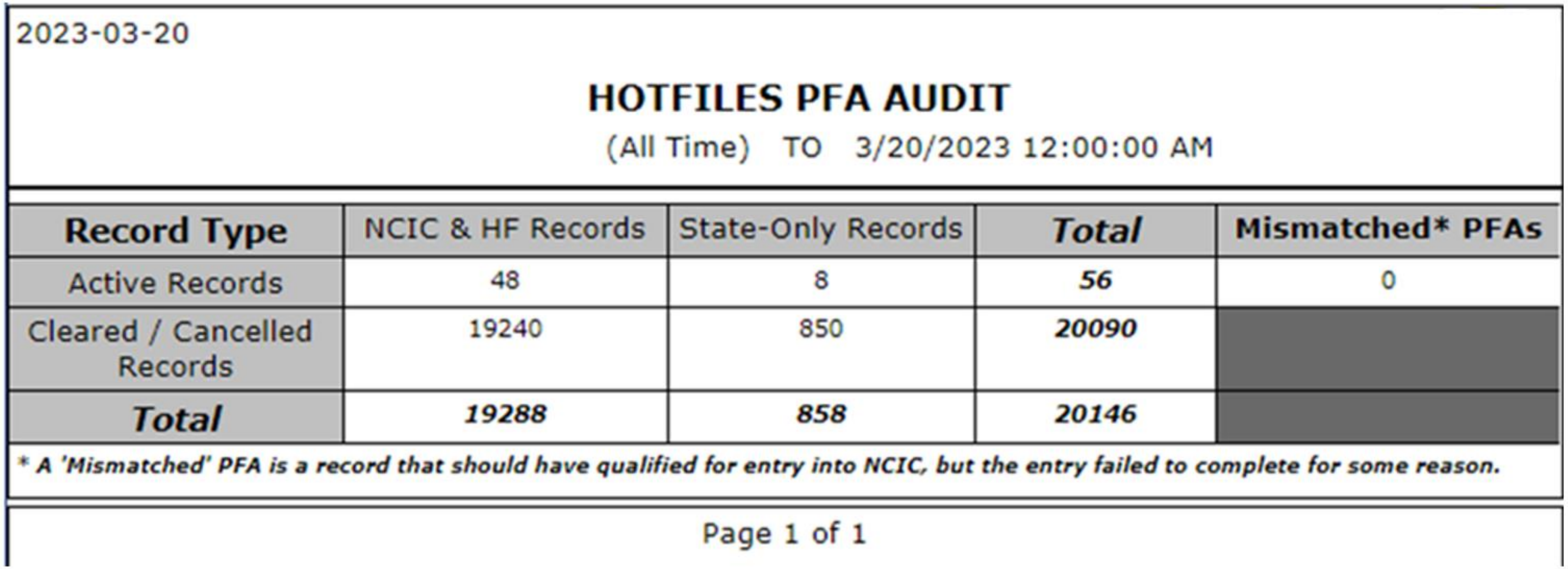
□ processing of a wanted person into Nebraska's hot file system

DEMO

Scenario 5: Hot Files

Demonstrate / Present:

□ ability to run a report of hot files data (e.g., the number of open warrants from a specific ORI or statewide)



2023-03-20

HOTFILES PFA AUDIT

(All Time) TO 3/20/2023 12:00:00 AM

Record Type	NCIC & HF Records	State-Only Records	***Total***	**Mismatched* PFAs**
Active Records	48	8	***56***	0
Cleared / Cancelled Records	19240	850	***20090***	
Total	***19288***	***858***	***20146***	

** A 'Mismatched' PFA is a record that should have qualified for entry into NCIC, but the entry failed to complete for some reason.*

Page 1 of 1

Scenario 5: Hot files

Demonstrate / Present:

- ☑ general hot file maintenance solution proposed for the system
- ☑ entry of a general wanted person record into the system, both via a command line and the GUI
- ☑ processing of a wanted person entry into NCIC, and include a demonstration of how the wanted person entry generates specific types of messages through the system
- ☑ ability to run a report of hot files data (e.g., the number of open warrants from a specific ORI or statewide)
- ☑ utilization of user-based roles or permissions associated with the hot file maintenance solution
- ☑ following hot file record queries:
  - Query wanted person (QW)
  - Registration query (RQ)
  - Query all state warrants (QWA)
- ☑ processing of a towed vehicle entry into Nebraska's hot file system
- ☑ processing of a wanted person into Nebraska's hot file system

Additional Presentation Topics

06

unisys

Additional Topics

Compliance and Strategy:

□ FBI Criminal Justice Information Services Security Policy Compliance – Please explain how the proposed MSS environment is compliant with the key aspects of this policy including network, system, data, and user security. entry of a general wanted person record into the system, both via a command line and the GUI

□ MSS Application Support – Explain how the proposed MSS application will be supported and upgraded over the life of the contract while ensuring NSP-specific code customizations/interfaces remain intact.

□ MSS Hardware/Software Interoperability – Explain how the proposed MSS environment is designed to allow for hardware and software upgrades/replacements without affecting the application.

□ Integration With Current Environment – Explain how the NSP solution will integrate with the current environment and other related applications.

□ Certification Tracking – Describe how the NSP solution will integrate with the Peak Performance user certification program and describe how certifications will relate to user authorizations in the new environment.

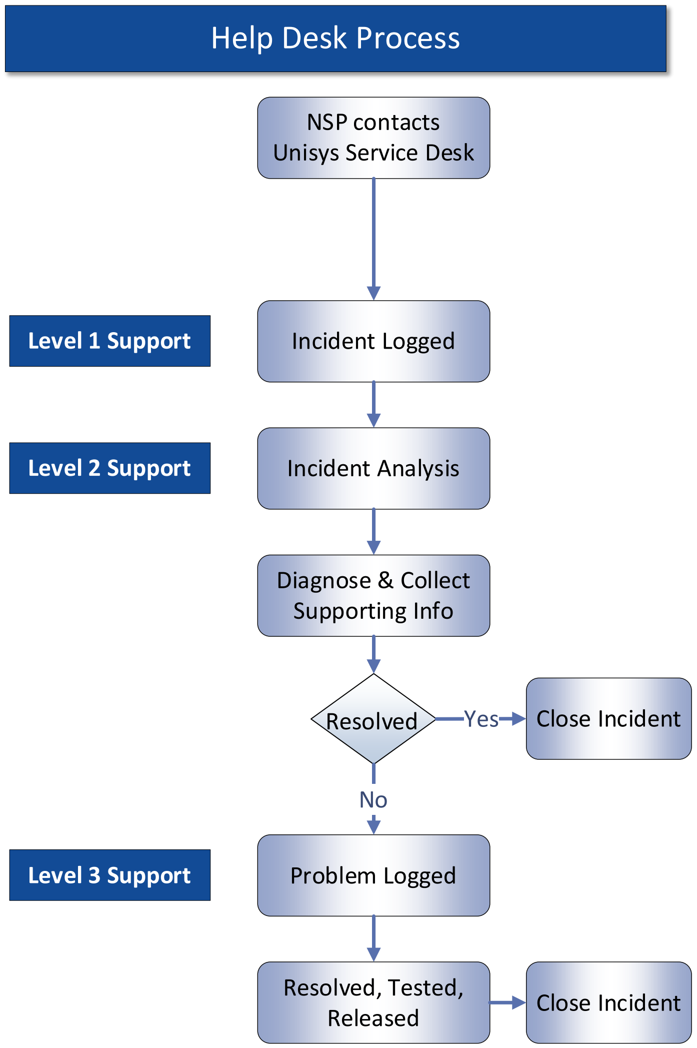
□ MSS Migration – Elaborate on your strategy to migrate to the proposed new environment while minimizing the impact to the operational production environment.

□ Available MKEs – Please discuss what MKEs are currently available in your proposed solution in comparison to the current Nebraska MKEs, placing particular focus on the activities necessary to bring the bidder's product into compliance with Nebraska's current MKEs, including those used by the State of Nebraska only.

FBI Criminal Justice Information Services Security Policy Compliance

- Explain how the proposed MSS environment is compliant with the key aspects of this policy including network, system, data, and user security
- The MSS solution complies with the FBI CJIS Security Policy (CJISSECPOL v5.9.1) in force at the time of RFP release for policy requirements applicable to an MSS
  - Policy Area 4: Auditing and Accountability
  - Policy Area 5: Access Control
  - Policy Area 6: Identification and Authentication
  - Policy Area 7: Configuration Management
  - Policy Area 8: Media Protection
  - Policy Area 9: Physical Protection
  - Policy Area 10: System and Communications Protection and Information Integrity

MSS Application Support – Service Desk



Help Desk Process

NSP contacts Unisys Service Desk

Level 1 Support — Incident Logged

Level 2 Support — Incident Analysis

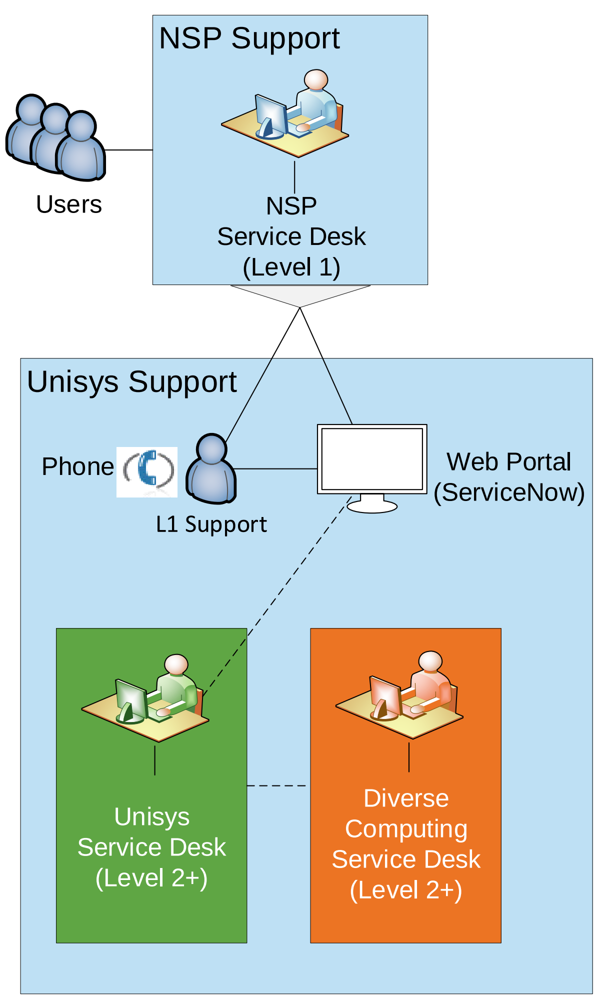
Diagnose & Collect Supporting Info

Resolved — Yes → Close Incident

No

Level 3 Support — Problem Logged

Resolved, Tested, Released → Close Incident



NSP Support

Users

NSP Service Desk (Level 1)

Unisys Support

Phone

L1 Support

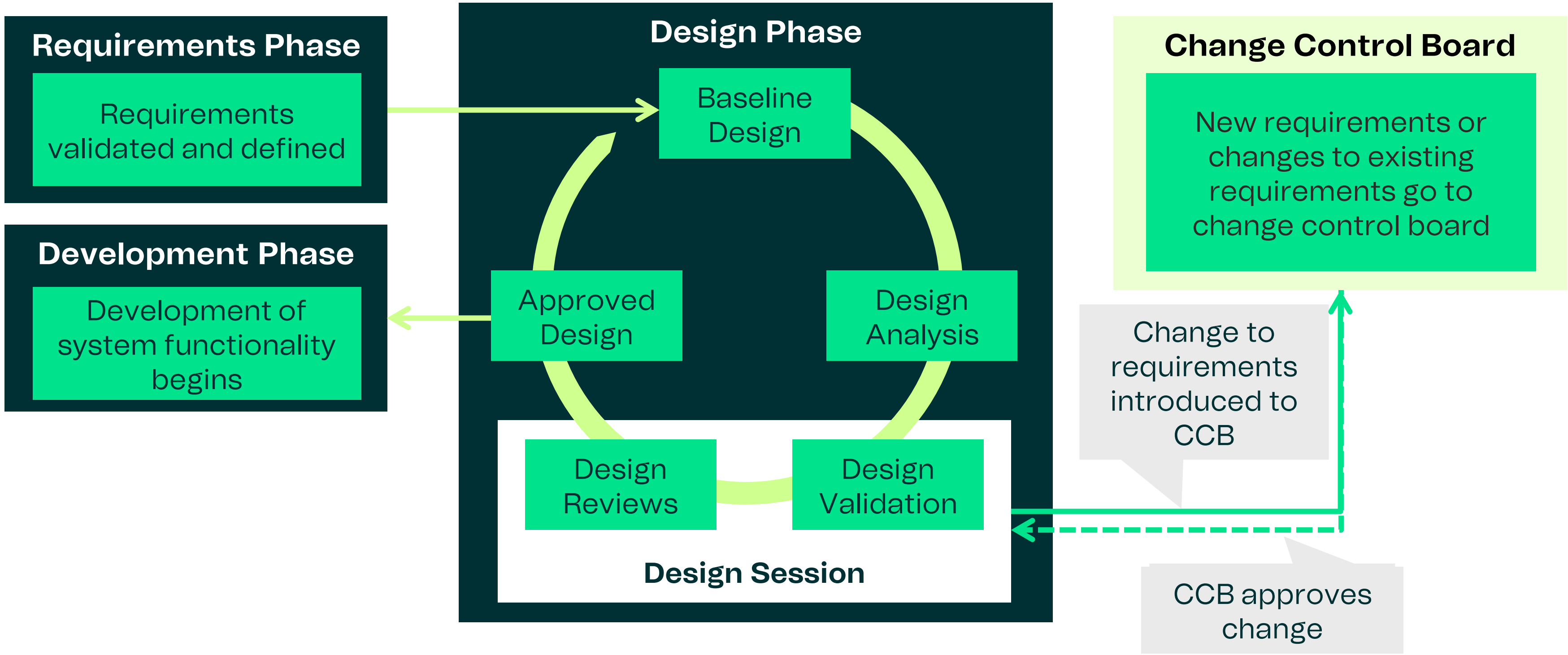
Web Portal (ServiceNow)

Unisys Service Desk (Level 2+)

Diverse Computing Service Desk (Level 2+)

MSS Application Support

Configuration Management / Change Control



Requirements Phase

Requirements validated and defined

Development Phase

Development of system functionality begins

Design Phase

Baseline Design

Design Analysis

Design Validation

Design Reviews

Approved Design

Design Session

Change Control Board

New requirements or changes to existing requirements go to change control board

Change to requirements introduced to CCB

CCB approves change

MSS Hardware/Software Interoperability

- Explain how the proposed MSS environment is designed to allow for hardware and software upgrades/replacements without affecting the application
- Hardware upgrades are performed by Microsoft as needed – deployed Azure infrastructure resources (VMs, disk storage, etc.) are automatically and silently transferred to upgraded hardware
- All Azure VMs running MSS components are load balanced or failover clustered to allow for software upgrades (such as operating system patches and application version upgrades) with only very brief or no user impact
- Software upgrades are performed at planned time during off hours
- Software upgrades are deployed to the test environment and tested prior to deploying to the production environment

Integration With Current Environment

- Explain how the NSP solution will integrate with the current environment and other related applications
- The solution will be configured to integrate with the current environment with only brief impact to the current environment
  - NCIC NIEM web services, III web services, and NICS NIEM web services will be deployed and verified independent of the existing MSS connection to NCIC TCP/IP sockets and will be switched from the current environment to the new environment at cutover
  - Nlets NIEM web services will be deployed and verified independent of the existing MSS connection to Nlets using a range of ORIs used for verification and will be switched from the current environment to the new environment at cutover
  - Interfaces to state systems will be implemented to comply with the current environment interface specifications and will be switched from the current environment to the new environment at cutover
  - Interfaces to local agency systems will be implemented to comply with the current environment DMPP/OFML specifications and will be switched from the current environment to the new environment at cutover; the new MSS LEMS Web Services will also be available at cutover
  - The Hot Files will be switched from the current environment to the new environment with migrated data at cutover
  - The User Interface will be switched from the current environment to the new environment (eAgent 2.0) at cutover
  - There is no anticipated need for interface with the current MSS or parallel operation of the new and current MSS

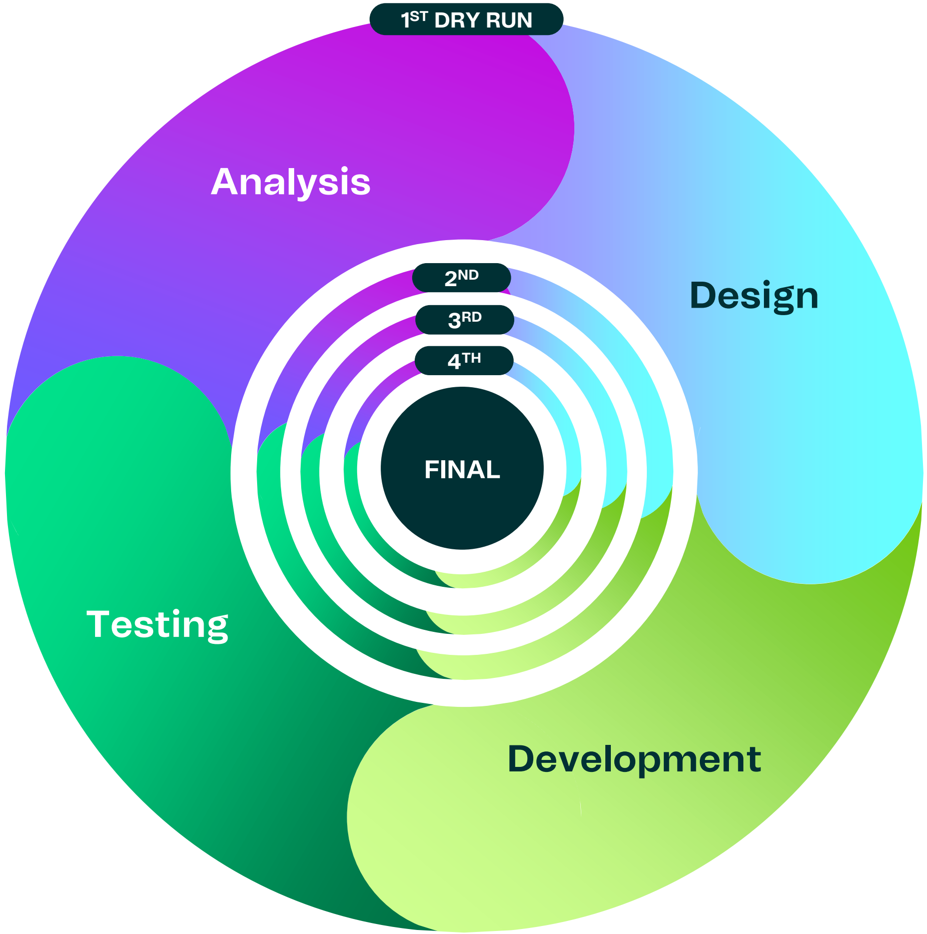
Certification Tracking

- Describe how the NSP solution will integrate with the Peak Performance user certification program and describe how certifications will relate to user authorizations in the new environment
- The solution will integrate with the Peak Performance nexTEST user certification program using LEMS Web Services in accordance with interface specifications agreed to by Unisys and Peak Performance as currently used in other states
- nexTEST retrieves user information from LEMS/JX over the interface
- When a user passes an authorized test, nexTEST sends the certification information to LEMS/JX to update the user’s function group (role permissions) and certifications date

MSS Migration

Data Migration

Data Conversion Planning →

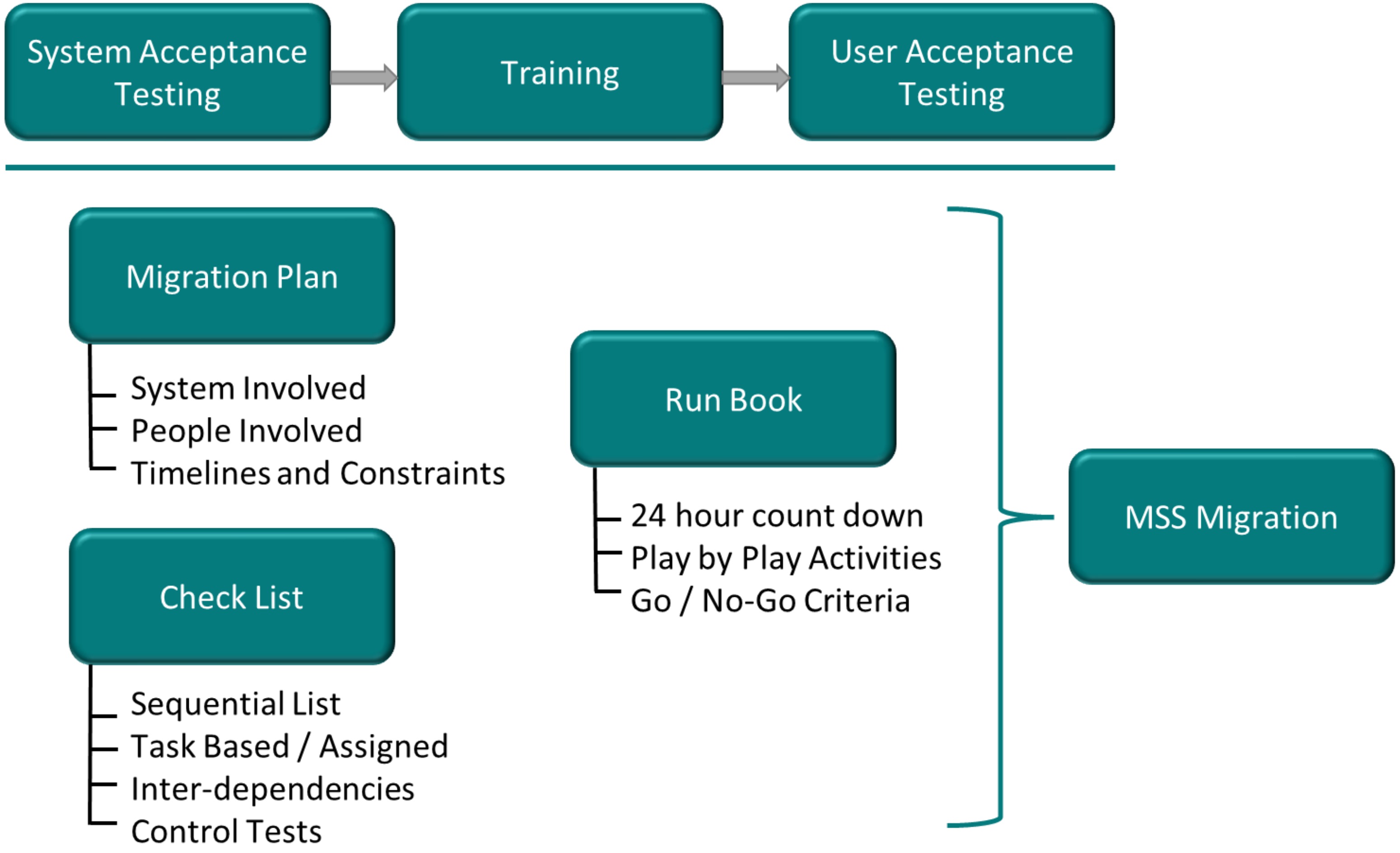


→ Go Live

MSS Migration

Migration Process

High Level Implementation



System Acceptance Testing → Training → User Acceptance Testing

Migration Plan
- System Involved
- People Involved
- Timelines and Constraints

Check List
- Sequential List
- Task Based / Assigned
- Inter-dependencies
- Control Tests

Run Book
- 24 hour count down
- Play by Play Activities
- Go / No-Go Criteria

MSS Migration

Available MKEs

Standard for LEMS

- All NCIC MKEs
- All III MKEs
- All NICS MKEs
- All Nlets MKEs, including
  - National Drug Pointer Index System (NDPIX) MKEs
  - National Insurance Crime Bureau (NICB) MKEs
  - Canadian MKEs
  - Interpol MKEs

Configure for NSP MSS

- CLEIN MKEs
  - Administrative
  - Criminal History
  - RITS
  - Stolen Vehicle/Parts
  - Towed Vehicle
  - Wanted Person
  - Internal
  - In-State Gun Check

Retired MKEs

- Obsolete and no longer supported by III, such as:
  - $.A.AFC
  - $.A.FNC
  - $.A.FCC
  - $.A.NAC
- No longer supported by NCIC in NIEM XML, as referenced in NCIC TOU 22-3

Additional Topics

Compliance and Strategy:

- ☑ FBI Criminal Justice Information Services Security Policy Compliance – Please explain how the proposed MSS environment is compliant with the key aspects of this policy including network, system, data, and user security. entry of a general wanted person record into the system, both via a command line and the GUI

- ☑ MSS Application Support – Explain how the proposed MSS application will be supported and upgraded over the life of the contract while ensuring NSP-specific code customizations/interfaces remain intact.

- ☑ MSS Hardware/Software Interoperability – Explain how the proposed MSS environment is designed to allow for hardware and software upgrades/replacements without affecting the application.

- ☑ Integration With Current Environment – Explain how the NSP solution will integrate with the current environment and other related applications.

- ☑ Certification Tracking – Describe how the NSP solution will integrate with the Peak Performance user certification program and describe how certifications will relate to user authorizations in the new environment.

- ☑ MSS Migration – Elaborate on your strategy to migrate to the proposed new environment while minimizing the impact to the operational production environment.

- ☑ Available MKEs – Please discuss what MKEs are currently available in your proposed solution in comparison to the current Nebraska MKEs, placing particular focus on the activities necessary to bring the bidder's product into compliance with Nebraska's current MKEs, including those used by the State of Nebraska only.

Lunch

07

unisys

Hot Files and General Topics

Compliance and Strategy:

□ Hosting Hot Files at NCIC – Please elaborate on your experiences with other clients in terms of hosting hot files at NCIC as opposed to the state repository.

□ Hosting Hot Files at Hosting Site/State Repository –Elaborate on your experiences with other clients in terms of hosting state-specific hot files at the proposed hosting site/state repository.

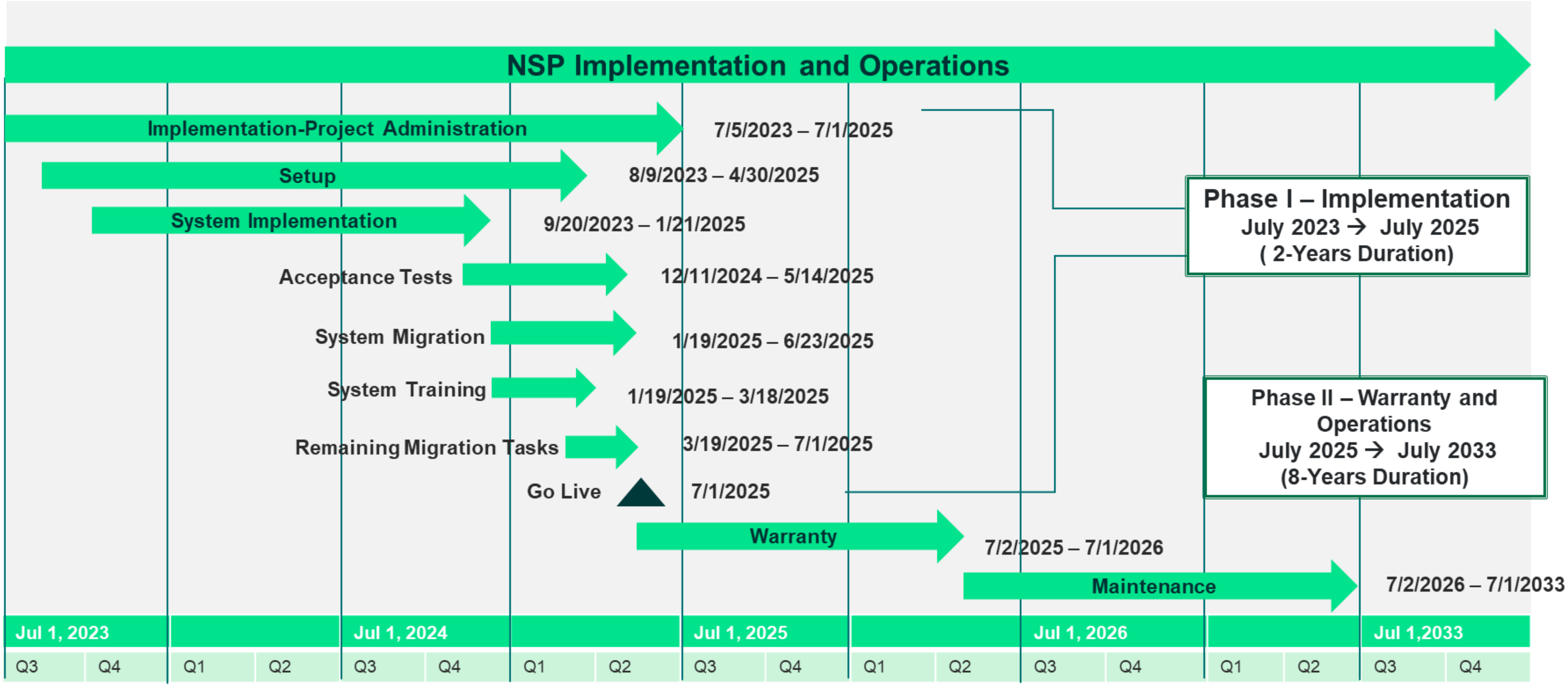
□ Project Overview – Please provide an overview of the project roadmap, delivery schedule, and initial project plan.

□ Customized Functions – For those requirements where the bidder indicated that the solution would meet the requirement through customized functions, describe the modification to the solution and its approach for delivering the required functionality.

Hosting Hot Files at NCIC vs. Hosting at Site/State Repository

- The Unisys State hot files solution is a framework that allows us to efficiently develop and maintain State hot files
  - Separate application loosely coupled to LEMS/JX using secure web services
  - Configurable/customizable business rules and workflows
- Reasons states host hot files at their hosting site/state repository
  - A need for a hot file not maintained by NCIC
  - Entry criteria that differs from that of NCIC
  - Additional fields beyond those maintained by NCIC
  - A need for hot file reporting capabilities beyond those offered by NCIC
  - Can be synced from State to NCIC where needed/appropriate
- Reasons states host hot files at NCIC
  - Reduces State footprint, deployment complexity, and costs that would otherwise be needed for State hot files
  - NCIC is highly available and responsive (wasn’t always that way)
  - Obviates the need to sync State hot file to NCIC or to modify State hot file design to keep up with NCIC hot file design
  - Doesn’t meet the criteria for hosting at hosting site/state repository

Project Overview – Delivery Schedule



NSP Implementation and Operations

Implementation-Project Administration 7/5/2023 – 7/1/2025

Setup 8/9/2023 – 4/30/2025

System Implementation 9/20/2023 – 1/21/2025

Acceptance Tests 12/11/2024 – 5/14/2025

System Migration 1/19/2025 – 6/23/2025

System Training 1/19/2025 – 3/18/2025

Remaining Migration Tasks 3/19/2025 – 7/1/2025

Go Live 7/1/2025

Warranty 7/2/2025 – 7/1/2026

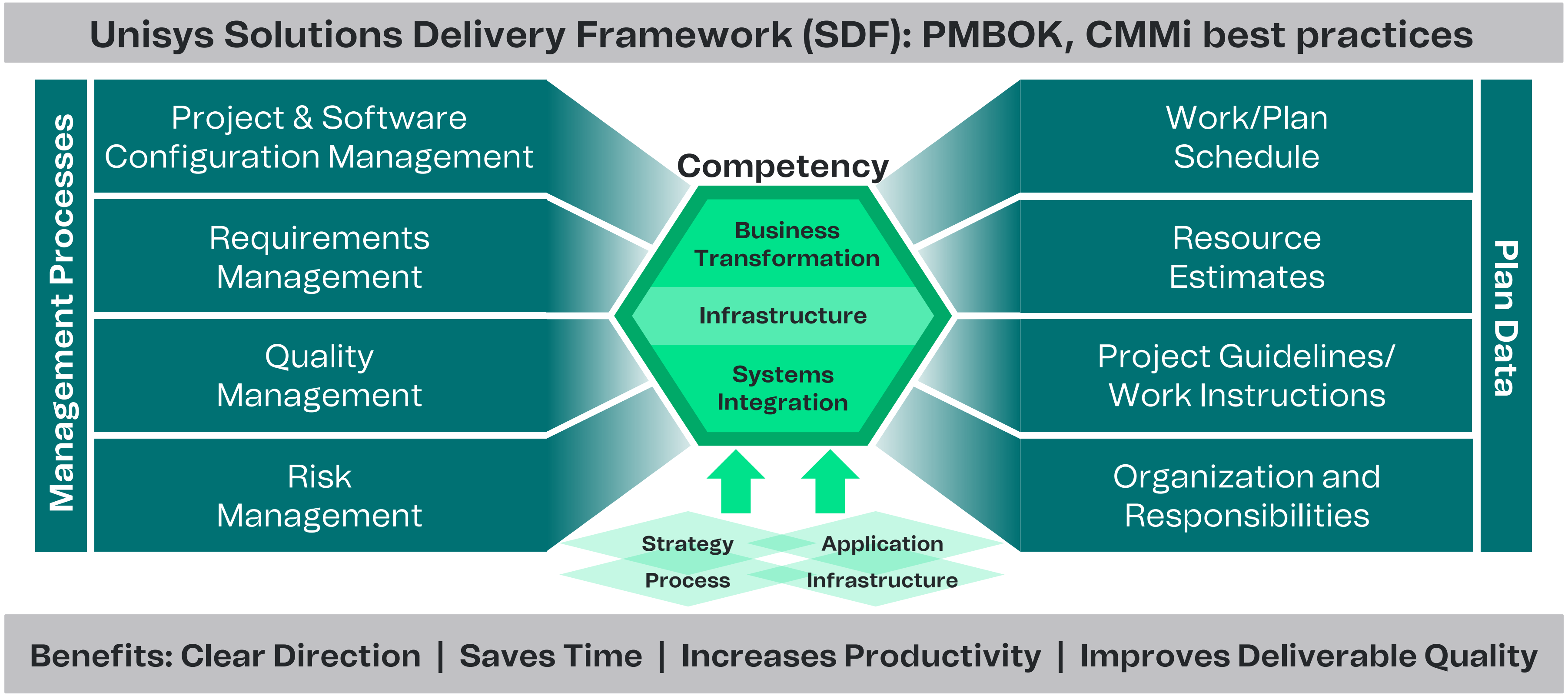
Maintenance 7/2/2026 – 7/1/2033

Phase I – Implementation
July 2023 → July 2025
(2-Years Duration)

Phase II – Warranty and Operations
July 2025 → July 2033
(8-Years Duration)

Jul 1, 2023				Jul 1, 2024				Jul 1, 2025				Jul 1, 2026				Jul 1,2033	
Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

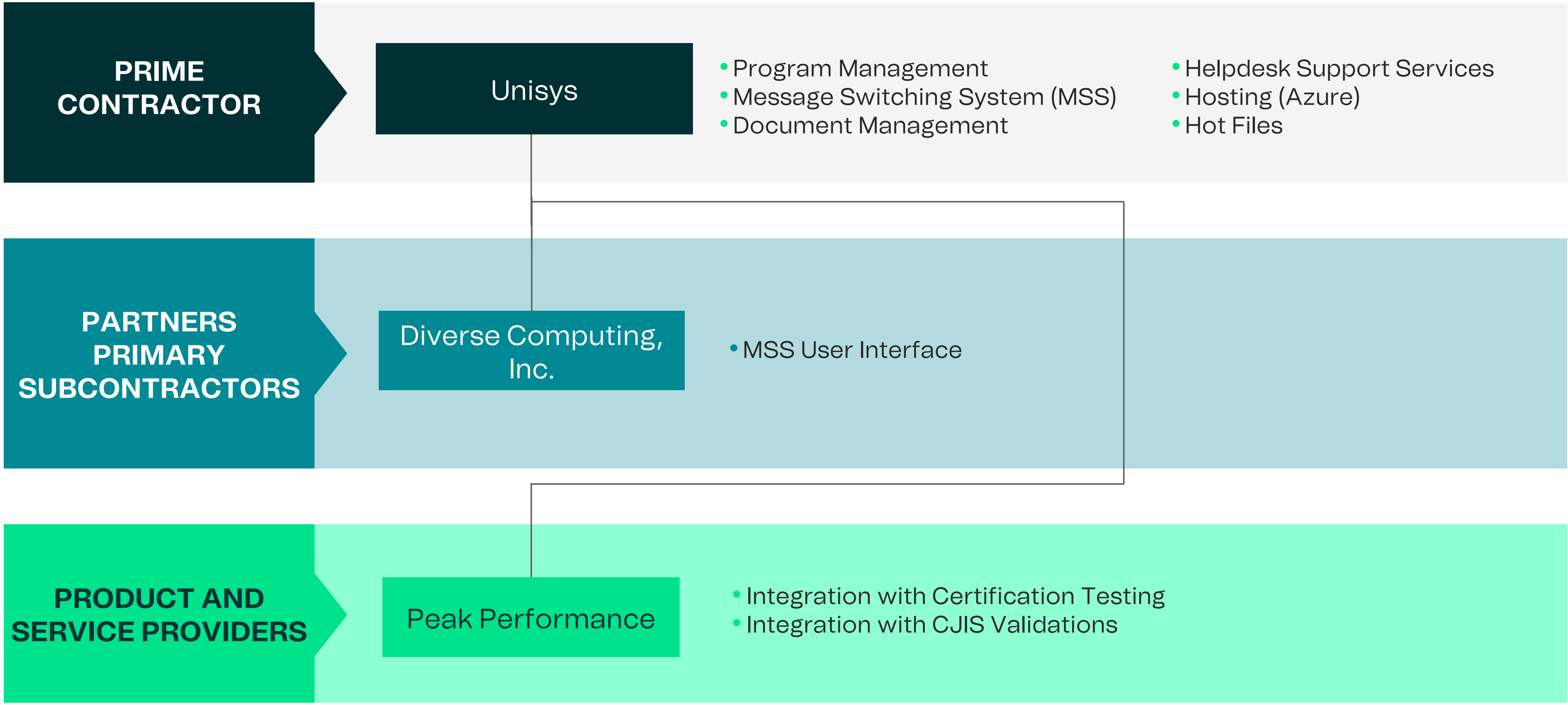
Project Overview – Project Management Planning



Unisys Solutions Delivery Framework (SDF): PMBOK, CMMi best practices

Benefits: Clear Direction | Saves Time | Increases Productivity | Improves Deliverable Quality

Project Overview – Initial Project Plan – Project Team



PRIME CONTRACTOR

Unisys

- Program Management
- Message Switching System (MSS)
- Document Management
- Helpdesk Support Services
- Hosting (Azure)
- Hot Files

PARTNERS PRIMARY SUBCONTRACTORS

Diverse Computing, Inc.

- MSS User Interface

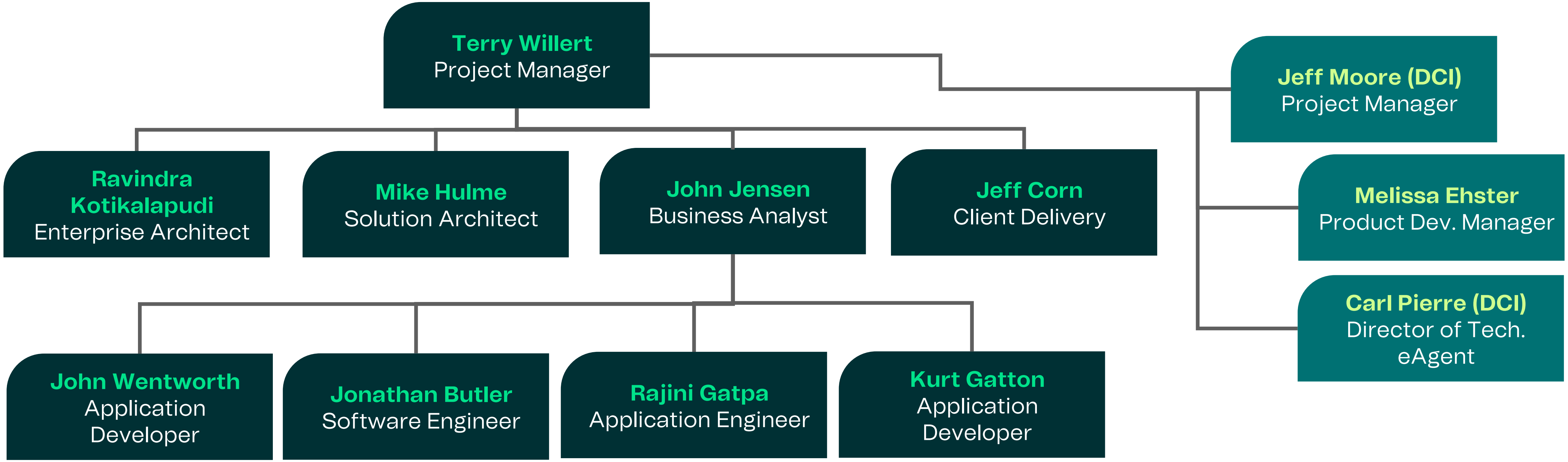
PRODUCT AND SERVICE PROVIDERS

Peak Performance

- Integration with Certification Testing
- Integration with CJIS Validations

Project Overview – Initial Project Plan

Leadership and Organizational Structure



Terry Willert
Project Manager

Ravindra Kotikalapudi
Enterprise Architect

Mike Hulme
Solution Architect

John Jensen
Business Analyst

Jeff Corn
Client Delivery

John Wentworth
Application Developer

Jonathan Butler
Software Engineer

Rajini Gatpa
Application Engineer

Kurt Gatton
Application Developer

Jeff Moore (DCI)
Project Manager

Melissa Ehster
Product Dev. Manager

Carl Pierre (DCI)
Director of Tech. eAgent

Customized Functions

□ Customized Functions – For those requirements where the bidder indicated that the solution would meet the requirement through customized functions, describe the modification to the solution and its approach for delivering the required functionality.

Hot Files and General Topics

Compliance and Strategy:

- ☑ Hosting Hot Files at NCIC – Please elaborate on your experiences with other clients in terms of hosting hot files at NCIC as opposed to the state repository.
- ☑ Hosting Hot Files at Hosting Site/State Repository –Elaborate on your experiences with other clients in terms of hosting state-specific hot files at the proposed hosting site/state repository.
- ☑ Project Overview – Please provide an overview of the project roadmap, delivery schedule, and initial project plan.
- ☑ Customized Functions – For those requirements where the bidder indicated that the solution would meet the requirement through customized functions, describe the modification to the solution and its approach for delivering the required functionality.

Wrap Up and Closing Comments

08

unisys

Thank you