



California
DEPARTMENT OF TECHNOLOGY
Office of Technology Services

Quarterly Network Forum

September 10, 2015



Opening and Introduction

Barbara Garrett
Deputy Director

**Statewide Telecommunications and Network Division
(STND)**



Agenda

- **9:00 – 9:10 AM** **Opening and Introductions**
Barbara Garrett – STND Deputy Director
- **9:10 – 9:20 AM** **Information Sharing**
Brian Parks – Network Engineering Branch Manager
- **9:20 – 9:40 AM** **Network Infrastructure Changes**
Gregory Parks – Projecting Engineering Unit Supervisor
- **9:40 – 9:55 AM** **Break (15 minutes)**
- **9:55 – 10:15 AM** **Security**
David Langston – Security Management Branch Manager
Shera Mui – Network Applications Section Manager
- **10:15 – 10:35 AM** **CGEN**
Brian Parks – Network Engineering Branch Manager
Mehdi Ghomeshi – CGEN Services Section Manager
- **10:35 – 10:50 AM** **CALNET**
Jann Biggs – CALNET Program Branch Manager
- **10:50 – 11:00 AM** **Q & A / Closing**
Barbara Garrett – STND Deputy Director



**Statewide
Telecommunications
and Network Division
(STND)**

Barbara Garrett
Deputy Director
Statewide Telecommunications
and Network Division (STND)

Brian Parks
DPM IV
Network Engineering
Branch

Jann Biggs
DPM IV
CALNET Program Branch

Maujala Price
DPM III
Network Engineering

Cindy Sherrets
DPM III
Network Infrastructure

Mehdi Ghomeshi
DPM III
CGEN Services Section

Vacant
DPM II
STND Business Support
Section

Calvin McGee
DPM II
CALNET Contract Services
Section

Elke Kleinke
DPM II
CALNET Program
Oversight Section

Caroline Lim
SSS III (Sup)
Network Management

Rich Hall
DPM II
Network Implementation

Scott Murray
DPM II
Network Capacity

Gary Jellis
SSS III (Sup)
Enterprise Engineering

Eric Gaines
DPM II
Network Projects

Gregory Parks
SSS III (Sup)
Project Engineering

Vacant
DPM I
Network Services



Information Sharing

Brian Parks
Manager

Network Engineering Branch



Level 3 owned IP address space

- OTech has removed Level 3 address space from the OTech core network, DNS and TMS-P
- We are very close to migrating CSLB and CalEPA
- We have met with DFW and DMV
- The migration team has initiated dialog with OES and DSH
- The purpose of this project is to migrate from vendor owned IP addressing
 - Risk: This address space can be reclaimed by the vendor at any time
 - Mitigation: OTech is collaborating with Level 3 to ensure adequate time to migrate



Super Sunday and PM Windows

- **Work completed during the last 3 Super Sundays**
 - **8/9/15:**
 - Remediate IKEv2 DOS vulnerability on VPN concentrators
 - Raised floor defragmentation – 2 Core routers moved
 - CGEN – 2 AT&T cards installed to support new, higher bandwidth lower cost host circuits



Super Sunday and PM Windows

■ 7/19/15:

- Raised floor defragmentation – 2 Core routers moved
- Upgraded software on firewalls in TMS Premium
- Migrated from Level 3 addresses for TMS-P

■ 6/14/15:

- Upgrade TMS-P switches in Pods 1 and 3
- Raised floor defragmentation – moved several data center routers, upgraded code, enabled SSH and disabled telnet



Super Sunday and PM Windows

- **Typical work completed during normal network PM windows**
 - Refresh of data center network hardware
 - Increases of capacity (bandwidth, port density, etc)
 - Network device software upgrades
 - Security patching
 - Implementation of new features/functionality
 - Break/fix that can wait for a PM window
- **Thank all of you for your willingness and flexibility to allow us to complete this work**



Decommission of CSGnet POP Sites

■ POP Sites that have been Decommissioned

- San Francisco
- Oakland
- San Diego
- Stockton
- Fresno
- Bakersfield
- Rancho Cordova
- DOF



Decommission of CSGnet POP Sites

- **POP Sites Remaining to be Decommissioned**
 - **DMV – One connection left – In progress**
 - **Los Angeles – Relocating to Santa Ana - Target completion 2nd quarter of 2016**
 - **After migration is complete, Los Angeles will be decommissioned**



Migration of Microsoft ISA Proxy Services to OTech Server Load Balancing and Reverse Proxy Service

- Department of Technology currently uses Microsoft Internet Security Acceleration (ISA) services to protect your IT environment from Internet threats while allowing secure remote access to applications and data. ISA also provides load balancing capabilities to multiple back end web farms, if required.
- To provide improvements to load balancing services, the Department of Technology is migrating to a more current method: Server Load Balancing/Reverse Proxy service.
- All migrations from ISA to the Server Load Balancing/Reverse Proxy service will be completed by April 1, 2016
- Customers should submit a Service Request (SR) for the migration from ISA to the Server Load Balancing/Reverse Proxy service.



Network Infrastructure Changes

Gregory Parks

Supervisor

Project Engineering Unit



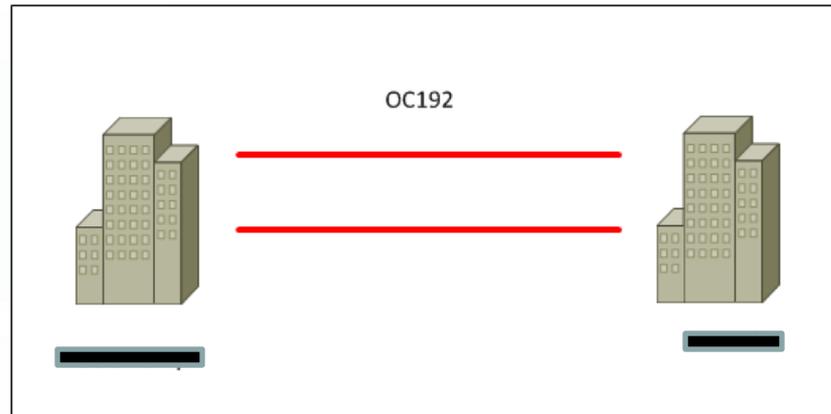
Data Center to Data Center Diverse Path

- **Dual Data Centers in Rancho Cordova and Vacaville**
- **Operational and Disaster Recovery**
- **Replication**
- **Storage**
- **Network Resiliency**
- **Virtual Machine Mobility**
- **Active – Active Services**
- **High Bandwidth**



Legacy Connectivity

- SONET, Optical Carrier lines
- Two redundant OC-192's at \$70,000 p/m



- Limited to 10 GB shared between all applications

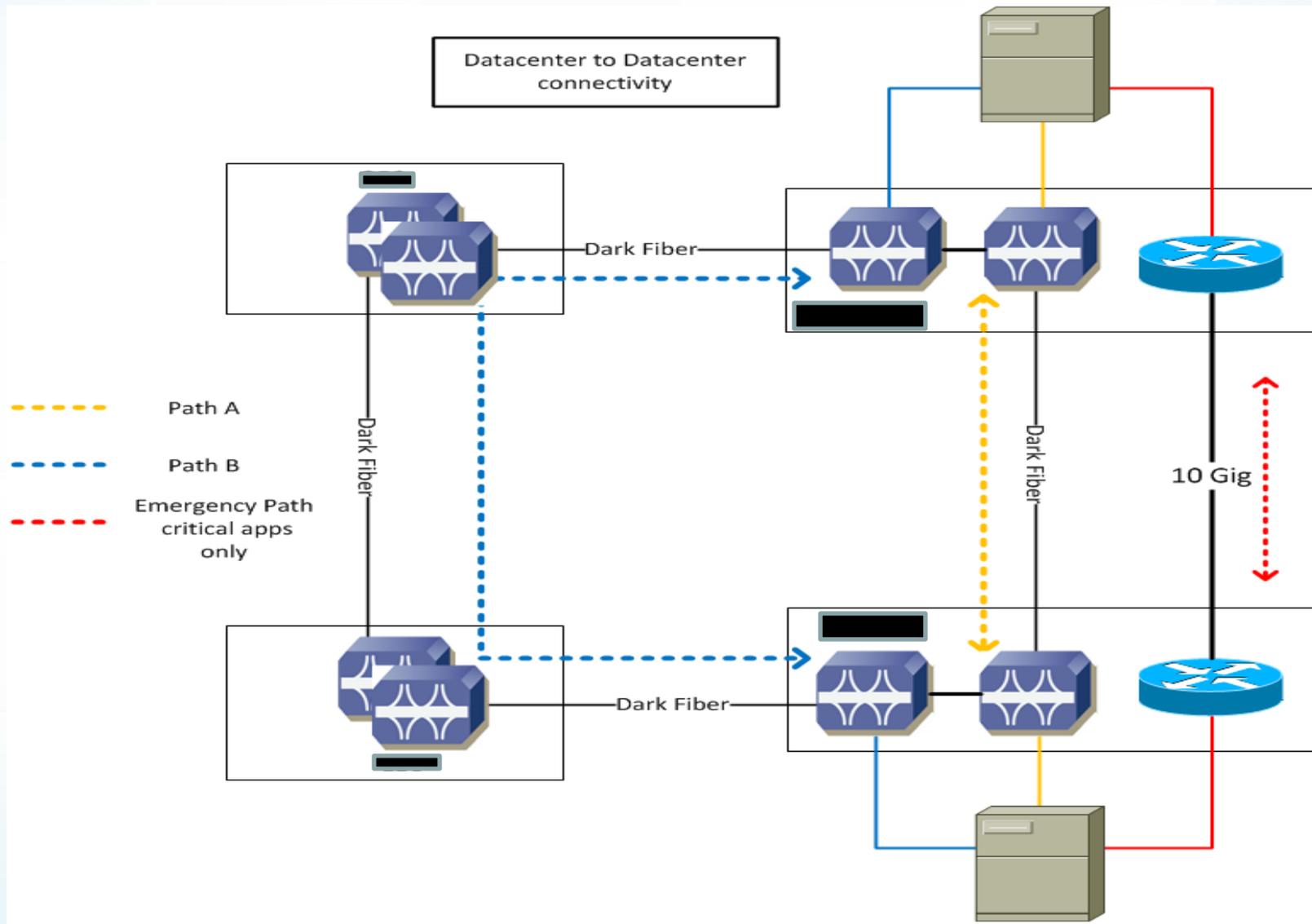


Dark Fiber Deployment

- Redundant entrance at Rancho Cordova
- Single entrance at Vacaville
- Fiber connects to downtown MAN Creating Fiber Ring Service
- 32 Wavelengths with 10GB capacity each dedicated
- 240GB Provision between the sites
- Replaced one OC-192 and three 1 Gig connections



Dark Fiber Deployment





Alternate Path

- **New path between Rancho Cordova and Vacaville 1Q**
2016
- **Encryption at Layer 1**
- **New chassis permits 100GB per wavelength**
- **40 Wavelengths**



Cost Savings and Avoidance

- The optical path replaced two OC-192 and three 1GB connections (\$91,000 per month)
- Currently Department of Technology have provisioned 240 GB between the sites. Thanks to this technology the dark fiber is avoiding \$720,000 monthly cost for equivalent bandwidth
- The Optical equipment has enabled encryption at L1 with minimum added cost
- 11 Month return on investment



Fiber Ring Services (FRS)

• What is new

- Fiber Ring Services no longer requires an exemption from CALNET
 - It has been incorporated into our CGEN service offering
- Additional access points in the Sacramento Metropolitan Area
 - OTech is adding approximately 15 more locations in the downtown area
- CALNET maintenance coverage for break/fix support

• What you may not know

- Redundancy for path, optical equipment, network, and power
- Complete access to datacenter services e.g. Internet, email, TMS, MCS, CalCloud, etc.
- 99.999% availability
- Bandwidth from 10MB to 10GB
- Managed and supported by OTech Network Engineering staff
- Protocols supported are: DWDM, Ethernet, MPLS, Fiber-channel



Fiber Ring Services (FRS)

On boarding process



- **How to request FRS services**

- **Downtown Fiber Ring Service**

- Step 1**

- Submit CSS request for Evaluation of service availability and Costs.

- Note:** This request will be closed after information has been provided.

- Step 2**

- Submit CSS to implement FRS Downtown connectivity, must attach cost proposal selected.

- **Data Center to Data Center**

- Step 1**

- Submit CSS to implement FRS Data Center to Data Center connectivity.



**Break
(15 minutes)**



Security

David Langston

Branch Chief

Security Management Branch



CalCloud Services

CalCloud is a suite of Cloud services offered by the Department of Technology, which includes:

- **Vendor Hosted Subscription Services (VHSS)**
- **Email**
- **Infrastructure as a Service (IaaS)**
 - **A private cloud infrastructure service hosted at the Office of Technology Services (OTech) data centers**



CalCloud Mission, Vision, Goal

■ Mission

- Offer cost-effective cloud solutions that will provide customers convenient, on-demand access to a shared pool of configurable resources.

■ Vision

- To be the catalyst for emerging new technology delivery models by delivering efficient, flexible, and secure cloud services to all customers.

■ Goal

- Drive customer adoption of CalCloud through new workload and business opportunities.

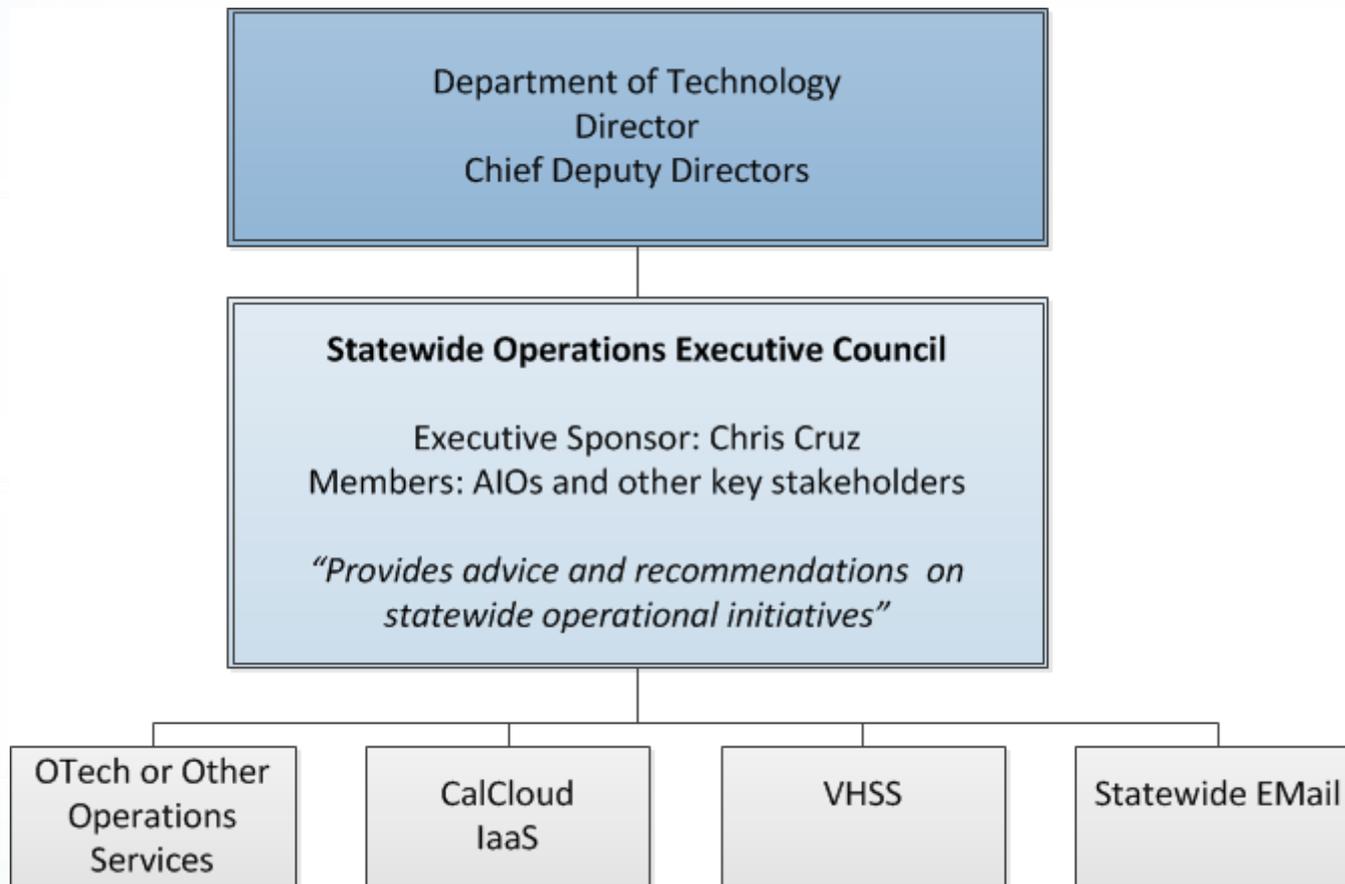


CalCloud Customer Benefits

- **Lower Cost Model**
- **Rapid Availability**
- **Secure Hosting**
- **Multiple Service Offerings**
- **Technology Recovery**
- **No Capital Expenditures**
- **Improved Flexibility**



Governance Framework





CalCloud Security

General

- **Provide services that meet the operational and compliance requirements of the State**
 - SAM/SIMM
 - NIST
 - FedRAMP where applicable
 - Other regulatory controls if/where applicable
- **Ensure that vendors are conforming to best security practices**



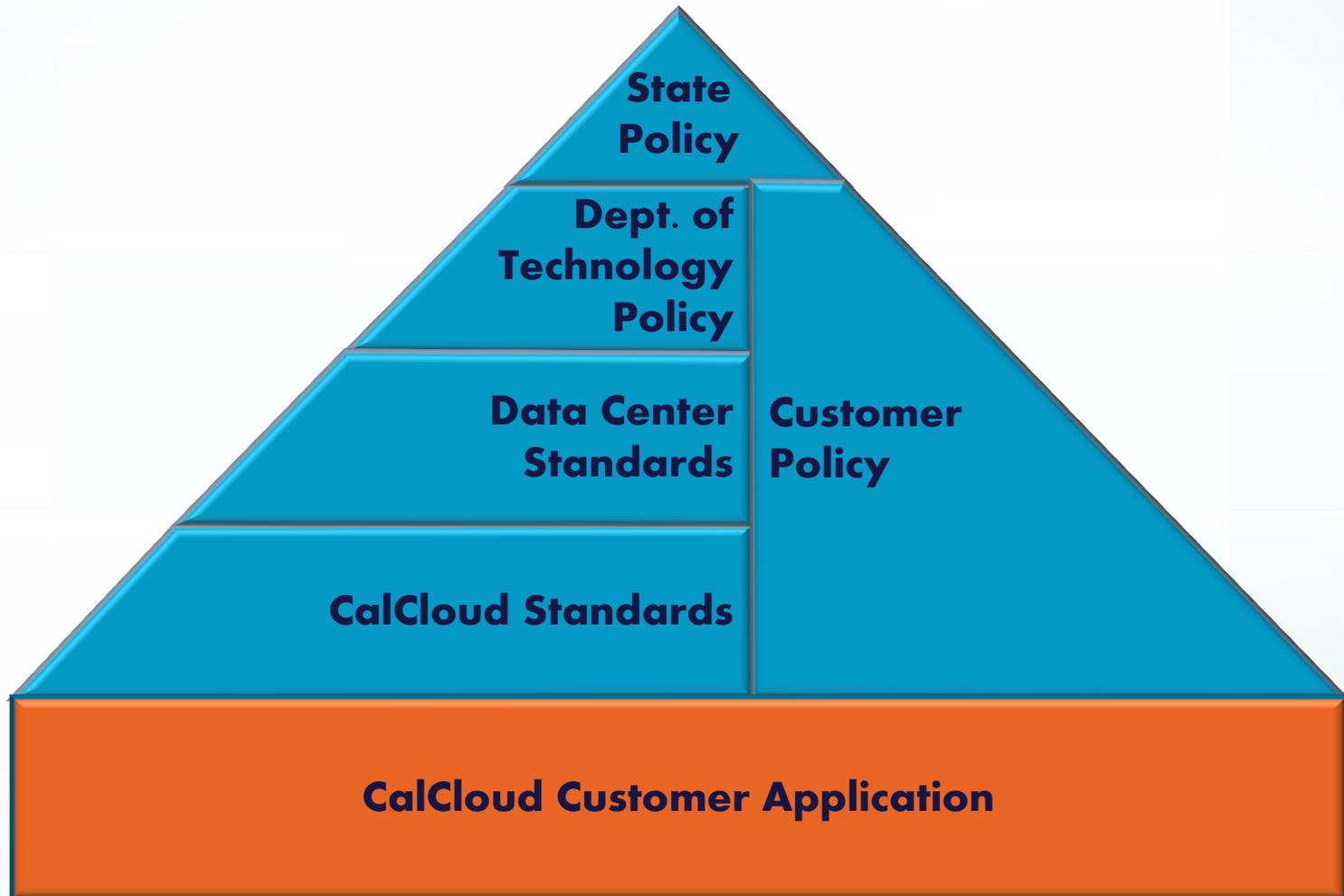
CalCloud IaaS Security

The goal of CalCloud IaaS is to deliver security that is equal to or better than security available in "dedicated" environments

- CalCloud IaaS environment was designed with security in mind
- Tenant isolation and zoning is key to the security model
- Best practices are used throughout the infrastructure
 - (e.g. two-factor authentication, least privilege practices, encryption options...)
- FedRAMP compliance is cornerstone to the security controls implemented
 - FedRAMP v2 in current implementation; redirection from v1 effort started early in 2015
- IBM projected compliance for FedRAMP, HIPAA, and IRS in September 2015

CalCloud IaaS Security

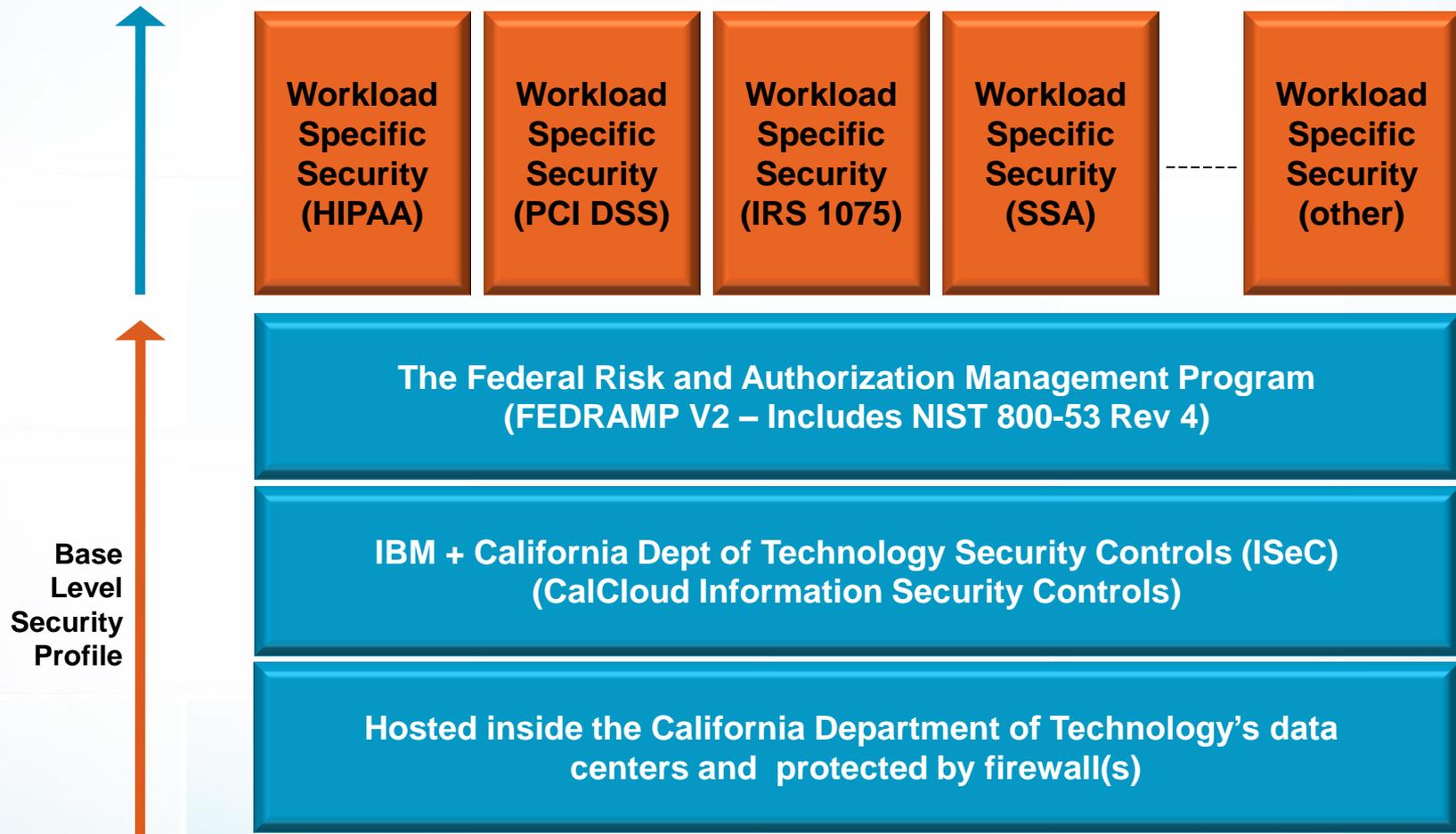
Policy Pyramid



CalCloud IaaS Security Stack



CalCloud provides a comprehensive and tiered security model





CalCloud IaaS Security Controls

- A formal security control program is in place (based on IBM ISeC processes, cloud experience, and FedRAMP V2)
- ~325 FedRAMP controls assessed against 25+ domains
- Compliance support to other authorities available (infrastructure controls only)
- CalCloud security controls can be shared with customer security personnel under strict controls and agreements

CalCloud IaaS Security

Key Elements



Encrypted Two-Factor Authenticated Sessions	Cloud Border Security	Admin Access Only from Territorial U.S.
Log of All Administrative Actions	Least Privilege and Separation of Duties Practice	Data are Property of the State
Infrastructure Hardening	Coordinated Security Incident Handling	Vendor(s) Background Checked
Encryption at Rest (Option)	Coordinated Change Control	Security Awareness Training Including IRS Disclosure
Strong Tenant Isolation	Coordinated OS Patching	No Shared Credentials
Isolated Security Tiers (network)	Configuration and Vulnerability Monitoring	Controlled Administrative Access



CalCloud IaaS Security

Then and Now

- 2014 1H focused on getting IBM ISeC in place
(this stood up the basic IBM processes for the environment)
- 2014 2H focused on FedRAMP v1 control implementation and processes
- Late 2014 FedRAMP focus switched to FedRAMP v2 (using NIST 800-53 v4 controls)
 - IRS had converted to NIST 800-53 v4 and customers need IRS compliance
 - IBM was moving other cloud infrastructures to FedRAMP v2
 - Decision to “bite the bullet”



Who is Using CalCloud IaaS Now?

CALIFORNIA DEPARTMENT OF
Health Care Services



CALIFORNIA DEPARTMENT OF
FOOD & AGRICULTURE



California Department of
Motor Vehicles



**CALIFORNIA EMERGENCY MEDICAL
SERVICES AUTHORITY**



CALIFORNIA
High-Speed Rail Authority



California
DEPARTMENT OF TECHNOLOGY

California Secretary of State



Security Enhancements for Mainframe Services

(Tech Alert 15-12)

Shera Mui
Manager

Network Applications Section



Why Secure Your Connections

As part of the Department of Technology's Security Enhancement Project, all existing Telnet (TN3270/TN3287) and FTP services will be migrated to secure/encrypted versions. This project is part of the strategic goal to mitigate potential threats and reduce risks to OTech hosted services, including all z/OS and mid-range server platforms.

- Communications that are sent in clear text can include usernames and passwords.
- Data being viewed or transmitted could potentially contain sensitive data like social security numbers and health records.
- Federal and control agency audits: Audit reports identify and red flag clear-text transmissions in violation of Federal and State laws and policies.
 - PCI (Payment Card Industry)
 - FTI (Federal Tax Information)
 - HIPPA (Health Insurance Portability and Accountability Act)



Security Enhancements

- **Transport Layer Security (TLS) has been enabled for FTP (FTPS) and Telnet (TN3270/TN3287) on the standard protocol ports of 21 and 23.**
- **A firewall request is not needed, if you have access to these ports today you will have access to the TLS version.**
- **You can change your session parameters to use TLS now, no need to delay or wait until the deadline.**
- **SSLv3 (Secure Socket Layer) has been disabled on port 21 and 23 to remediate the risk of the POODLE vulnerability, a man-in-the-middle exploit.**
- **Port 2121 (Current FTPS SSL/TLS-only) and port 2323 (SSL/TLS-only) will continue to be supported. SSLv3 support will be removed by January 2016.**



Does this affect me?

- Any FTP or Telnet (TN3270/TN3287) session to an OTech managed mainframe using port 21 or port 23. This includes Telnet print on port 23. Only inbound connections to the mainframe on port 21 or 23 are within the scope of the project.
- Any FTP transmissions to the mainframe FTP Server. Check your FTP desktop clients and batch jobs: do they target an OTech mainframe using port 21 in the software settings or job?



Preparing for the disabling of clear-text

- OTech will disable clear-text connections during a small window of time during production hours. The “test” will be coordinated and communicated in advance. On the day of the change clear-text will be disabled for only a short block of time, approximately 2.5 hours and the change will be rolled back.
 - Any individual Telnet user who has not enabled encryption and attempts a connection at this time will not be able to connect. Be aware, that connections made before the system is actually changed will remain connected and unaffected. Please have your users who are already connected, disconnect and reconnect at this time to perform the test.
 - If sessions have already been migrated to TLS there will no impact to those users.

- Action Requested:
 - Configure your sessions now for TLS, do not wait for the deadlines change. Once this done you do not need to worry about future deadlines.
 - All customers will be required to configure all Telnet sessions for port 23 to TLS. If your department does not believe they will be able to meet this requirement in a reasonable amount of time your department will need to file a standard security exemption.



Implementation Dates

- Due to complexity the customer shared mainframe environment we cannot at this time solidify drop dead dates for production shared systems. Some internal OTech and dedicated customer systems have been completed successfully and others will proceed forward.
 - **Telnet(TN3270/TN3287) Target Dates:**
 - Stage 1: SY9, SY0, Test, TST2, SY8 **COMPLETED**
 - Stage 2: SY4, SY6, SY7 **COMPLETED**
 - Stage 3: SY3 **COMPLETED**
 - Stage 4: SCT1, SCT2 (09/12/2015)
 - Stage 5: SOC (09/17/2015)
 - Stage 6: SOCP (09/27/15)
 - Stage 7: SY5 **TBD**
 - Stage 8: S1S1 **TBD**
 - Stage 9: S2S2 **TBD**

 - **FTP Target Dates:**
 - Stage 1: SY9, SY0, Test, TST2, SY8 **COMPLETED**
 - Stage 2: SY3 **TBD**
 - Stage 3: SY2, SY7 **TBD**
 - Stage 4: SY4, SY6 **TBD**
 - Stage 5: SCT1, SCT2 (10/10/2015)
 - Stage 6: SOC (10/15/2015)
 - Stage 7: SOCP (10/25/2015)
 - Stage 8: S1S1 **TBD**
 - Stage 9: SY5 **TBD**
 - Stage 10: S2S2 **TBD**



Contact Information

If you have questions or need further clarification regarding the project, please contact your Dept. of Technology Account Lead. If you are unsure who your Account Lead is, visit the account look-up page @ (<http://www.dts.ca.gov/Customers/default.asp>) or call the Customer Delivery Division at (916) 431-5476.

If you are trying to configure a TLS session and are having difficulties, contact the OTech Service Desk (Service.Desk@state.ca.gov or (916) 464-4311) and open a work order for assistance.



CGEN

Brian Parks

Manager

Network Engineering Branch



CGEN NextGEN Strategic Objectives

- **Manage the Host Shared Circuit Costs:**
 - New strategy cuts in half the cost of adding new CALNET Vendors
 - Allows more efficient use of the bandwidth
- **Simplify the Handoff Between Vendors and the State:**
 - WAN Routing to reach iHub or Department HQ managed by Vendors
 - Application routing to reach business destination managed by OTech
- **Improved Responsiveness to Customer Needs:**
 - Streamline Incident Management
 - Streamline Change Control



Shift in Edge Device Management

Current Situation OTech Templates

OTech dictated ACL & Protocols.

Site LAN Definition

State Legacy Network Protocols

State Program ACLs

Proposed Refinement: OTech Production Configurations

Site LAN Definition

State Legacy Network Protocols

State Program ACLs

OTech Overlay Definition

- 2 Stage Routing Plan
- Available Transport Encryption

Device Configuration

- Network Access Definition
- Network Management Definition
- Device IP Address

Device Vendor Software

Access Device

Access Circuit

■ **Orange Shading:**
OTech scripting with
vendor remote
hands

■ **Green Shading:**
Vendor provides the
initial configuration
and OTech controls
the complete
production
configuration file



Progress

- Working with CALNET contract administrators
 - Finalize OTech requirements
 - Determine what contract changes may be required
- Testing of Overlay technologies is complete
 - DMVPN was selected
 - Open Standard
 - Widely accepted
 - STND Network Engineers already experienced
- Initiate Proof of Concept



CGEN

Mehdi Ghomeshi

Manager

CGEN Services Section



CGEN Services Section

- **Migration of non-CGEN Customers**
- **Approach to migration to CGEN**
- **Benefits of CGEN**



Non-CGEN Customers by numbers

- **Estimated 15 customers**
- **Approximately 950 Circuits/ Connections**
- **CDCR, CHP, and Caltrans account for more than 600 Circuits/ Connections**



Approach

- Reach out to non-CGEN customers who are subject to AB 2408:
 - I. Develop customer profile – in collaboration with the customers
 - II. Review customer current Network Topology and configuration
 - III. Inquire and document their current business needs



Approach Cont'd

- IV. Schedule time to develop and design their To-Be configuration, in collaboration with the customers
- V. Collaborate and develop alternative solutions with the CALNET Vendors based on collected data
- VI. Develop cost estimates for alternatives and establish approximate time lines
- VII. Follow up meetings with customers to present solutions, estimated costs and time lines



Benefits of migrating to CGEN

- **Competitive rates**
- **Potential lower rates - more customers paying the infrastructure fee (iHub/Internet) could lead to lower costs**
- **Class of Service – smart network that allows traffic prioritization**
- **Multiple 10 GB connections**
- **Vendor diversity, OTech connects to Tier 1 ISP providers – 3 regionally diverse connections, 3 separate vendors**



Benefits of migrating to CGEN

- Public IP addresses provided
- Intrusion detection / prevention systems
- DDoS Mitigation
- Access to cloud based services
- Dedicated team with an effective escalation process
- And more..



Security Features of CGEN

- Network encryption capability
- Background checks
- Virtual Private Networks
- Customer administration of their own security policy
- Vendor compliance with security standards



CALNET

Jann Biggs
Manager

CALNET Program Branch



CALNET Topics

- **CALNET Contracts**
- **CALNET Program**



CALNET

Leveraged Procurement Agreement (LPA)

- **Competitively Bid, Multiple Award Contract**
 - Vendors must pre-qualify before competing
 - Vendors must agree to comprehensive business requirements, including Service Level Agreements
 - Vendors must agree to technical requirements
 - Competition drives lower pricing
- **Telecommunications and Network Services**
 - Voice Services
 - Data Services
 - Security Services
- **Collection of contracts**
 - Multiple categories
 - Multiple vendors
- **IFB = Invitation for Bid**



CALNET Categories

Categories 1.1-1.5, 11/15/13 – 6/30/18, with two 1 year extensions

Category 1.6, 11/15/13 – 6/30/17, with three 1 year extensions

Categories 2-7, 6/26/14 – 6/30/18, with two 1 year extensions

	IFB-A						IFB-B						
	<u>1.1</u>	<u>1.2</u>	<u>1.3</u>	<u>1.4</u>	<u>1.5</u>	<u>1.6</u>	<u>2</u>	<u>3</u>	<u>4.1</u>	<u>4.2</u>	<u>5</u>	<u>6.1</u>	<u>7</u>
	<u>1.1</u> Dedicated Transport	<u>1.2</u> MPLS C-VoIP	<u>1.3</u> VoIP	<u>1.4</u> Long Distance	<u>1.5</u> Toll-Free	<u>1.6</u> Legacy	<u>2</u> Web Conferencing	<u>3</u> MAN Ethernet		<u>4.2</u> SONET Point to Point	<u>5</u> Managed Internet	<u>6.1</u> Hosted IVR	<u>7</u> Network Based Managed Security
				<u>1.4</u> Long Distance	<u>1.5</u> Toll-Free		<u>2</u> Web Conferencing	<u>3</u> MAN Ethernet					<u>7</u> Network Based Managed Security
		<u>1.2</u> MPLS C-VoIP	<u>1.3</u> VoIP					<u>3</u> MAN Ethernet	<u>4.1</u> SONET Ring	<u>4.2</u> SONET Point to Point	<u>5</u> Managed Internet		
		<u>1.2</u> MPLS C-VoIP	<u>1.3</u> VoIP										
		<u>1.2</u> MPLS C-VoIP					<u>2</u> Web Conferencing					<u>6.1</u> Hosted IVR	
	<u>1.1</u> Dedicated Transport	<u>1.2</u> MPLS C-VoIP	<u>1.3</u> VoIP		<u>1.5</u> Toll-Free				<u>4.1</u> SONET Ring	<u>4.2</u> SONET Point to Point		<u>6.1</u> Hosted IVR	<u>7</u> Network Based Managed Security



Procurement vehicle

Streamlined process

- Customers can avoid running their own procurements
- Customers can leverage the work already done for CALNET
- Customers can evaluate multiple vendors for a particular service
- Services are readily available
- Requires only STD Form 20



CALNET Program

Pricing Advantages

- Most Favored Nation
- No dollar ceilings
- Postalized (Statewide) pricing
- Capped pricing with Individual Price Reduction (IPR) opportunities
- Continuous competition





CALNET Program

Vendor Management

- Constantly monitor the vendors for compliance to all contractual agreements
- Constantly monitor the vendors for quality performance
- Ensure SLA compliance and financial remedies

Customer Service

- Customer Service Line for support
 - Ensure customers know how to leverage the benefits of the CALNET Program
 - Customers can report issues with a vendor
 - Customers seek advice on CALNET services that might meet their business needs.





CALNET Program

Available to

- **State Government entities – mandatory use**
 - Chief Agency Telecommunications Representative - CATR
 - Agency Telecommunications Representative – ATR
- **Local Government entities – optional use**

Processes

- **CALNET Exemption Requests**
- **CALNET Delegation Requests**





CALNET Program

Contract Management

- Amend categories
- Add categories
- Individual Price Reductions
- Statements of Work
- Resolve customer billing issues
- Monitor SLAs and financial remedies



Future Categories

■ IFB – C: Category 10: Satellite



■ IFB – D: Category 12: Basic VoIP





CALNET Information

■ CALNET Website

<http://www.otech.ca.gov/stnd/calnet3/>

- Frequently Asked Questions

- Catalogs of Services

- Bulletins

- User Instructions

■ Vendor websites

- Listed on the CALNET site as links



Questions and Answers