



California
DEPARTMENT OF TECHNOLOGY

Vendor Forum

CDT Training and Education Center
October 17th, 2016

Introducing...

Chris Cruz

**Chief Deputy Director,
California Department of Technology**



California
DEPARTMENT OF TECHNOLOGY

Agenda

Opening Remarks

DGS Procurement Updates

- Cloud-based Cooperative Contracts
- Terms and Conditions for XaaS

Updates on Service Offerings

- CalCloud 3.0
- VHSS
- Security
- CALNET

Q&A





Introducing...

Jim Butler

Deputy Director,

Procurement Division

Department of General Services

Introducing...

Scott MacDonald

**Deputy Director,
CalCloud Services Division**



California
DEPARTMENT OF TECHNOLOGY

CalCloud 3.0

Business Requirements

Reducing Time to Value –

Ability to add new services to meet evolving needs.

Savings through Agility –

Driving efficiency through automation, flexibility, and portability.

Workforce Development –

Expanding opportunities for state employees through professional development and support transitioning.

Security Requirements

Protecting the State's Confidential/Sensitive Data –

Shared security services and threat identification.

Secure by Default –

Master service catalog and architectural patterns established by CDT.



CalCloud 3.0

Transition of many on-premise IaaS support services to state

- CDT to share support responsibilities by January 2017
- Continued partnership with IBM

Development of Workgroup to define CalCloud roadmap and prioritize objectives

- Gain representation from all key stakeholders (2016 Q4)

Enterprise Portal

- Interface into other CDT services



CalCloud 3.0

Moving to a hybrid community cloud service offering

Private (Community) Cloud provides the highest levels of management visibility, control, security, privacy, physical data proximity and levels of support. Private clouds are typically less susceptible to cyber-attacks.

Ideal for:

- Vertical specific application integration and compatibility
- Applications/systems containing confidential and sensitive information
- Complex environments requiring increased levels of support



Public Cloud is likely to be less expensive and offer a greater number of services; however offers limited troubleshooting support and transparency of security controls.

Ideal for:

- Test and development environments
- Non mission critical systems and data
- Cheap storage of non-confidential/sensitive data



CalCloud 3.0

Hybrid Community Cloud is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns – e.g., mission, security requirements, policy, and compliance considerations and may exist on and off premises.

Benefits of combining public and community cloud services:

- A holistic approach to the consumption of IT matching the right solution to the right job.
- Minimizes trade-offs and breaks down barriers to get the maximum benefit and improved performance, thereby driving the business forward
- Quantifiable cost benefits
- Combines agility and security

Data classification and system categorization will be a key factor in determining where systems and data resides.

- The protection of California's mission critical systems and confidential/sensitive data continues to be a key requirement.



CalCloud 3.0

Coming Soon*

(*Timelines to be further defined by workgroups.)

2017 Q1/Q2

- High Availability between data centers
- Service Level Agreements
- DevOps
 - Facilitates Agile Software Development
 - Support for containers
- Platform as a Service (PaaS)
- Enhanced security monitoring and integration with Cal-CSIC
- Database as a Service (DBaaS)
- Network Automation
 - User Provisioning of Firewall Rules
- Database Backup and Recovery Services
- Public/Private Hybrid Cloud
 - Ability to move workloads between environments
 - Secure Cloud Network Exchange

Introducing...

Richard Rogers

Deputy Director,
Engineering Division



California
DEPARTMENT OF TECHNOLOGY



Vendor Hosted Subscription Services (VHSS)

Current

- IT Service Management (ITSM)
- Customer Relationship Management (CRM)
- Project & Portfolio Management
- Email & Office Productivity: Office 365

In Development

- eSignature / Digital Signature
- Human Resource Tools
- Storage
- Business Intelligence
- Disaster Recovery



Introducing...

David Langston

**Manager,
Security Management Branch**



California
DEPARTMENT OF TECHNOLOGY

Security Monitoring Expansion Project (SME)

Project expands use of MSSP into CDT data centers and networks

3 Focus Areas

Security Information & Event Management (SIEM)

- Most services already sending logs
- Team now working to get closure on all sources
- Tuning will begin thereafter

Vulnerability Scanning/Management

- Initial scans are complete
- Conversion November 1st

Intrusion Detection/Protection

- MSSP assessing IPS configurations and operational model in October

Schedule

- Standup of all services and service areas EOY '16
- Tuning refinement completed June '17

Cal-CSIC integration dialogs in the works



Back to...

Scott MacDonald

California Information Security Office



California
DEPARTMENT OF TECHNOLOGY

Policy Modernization

| Function | 2016-2018 Priority Objectives |
|----------|--|
| | [MANAGE at this level] |
| IDENTIFY | <ul style="list-style-type: none"> - Application Inventory Management - Application Assurance Level Definition - Awareness Training Program - Application Assurance Level Definition - Comprehensive Security Policy Structure - Business Impact Assesemnt - Data Classification Policy and enforcement - Procurement and Acquisitions - Risk Acceptance - Security Management Plan - Comprehensive platform-specific vulnerability scanning process - Comprehensive vulnerability identification process including periodic production vulnerability scans for platform and applications |
| PROTECT | <ul style="list-style-type: none"> - Application Assurance Level Definition - Secure Code Practices - Comprehensive enterprise change management process, workflow, database - Embed formal security evaluation in enterprise CI process - Encryption of sensitive database fields - Platform-specific build standards and procedures - Platform-specific hardened standards and procedures - Comprehensive, documented enterprise process management and p - Multi-factor authentication for elevated risk use cases - Privileged user management and best practices enforcement - Enterprise mobile device management - Technical enforcement of security layers and Data center separation - Network Admission Control - Comprehensive platform-specific anti-malware approach - Physical security |
| DETECT | <ul style="list-style-type: none"> - Exposure and Enterprise sp |
| RESPOND | <ul style="list-style-type: none"> - Compreher |
| RECOVER | <ul style="list-style-type: none"> - Comprehensive DRP and Testing |

| No. | Control |
|-------|---|
| IR-1 | INCIDENT RESPONSE POLICY AND PROCEDURES |
| IR-2 | INCIDENT RESPONSE TRAINING |
| IR-3 | INCIDENT RESPONSE TESTING |
| IR-4 | INCIDENT HANDLING |
| IR-5 | INCIDENT MONITORING |
| IR-6 | INCIDENT REPORTING |
| IR-7 | INCIDENT RESPONSE ASSISTANCE |
| IR-8 | INCIDENT RESPONSE PLAN |
| IR-9 | INFORMATION SPILLAGE RESPONSE |
| IR-10 | INTEGRATED INFORMATION SECURITY ANALYSIS TEAM |

Comprehensive Incident Response Plan and Procedures

- 28 security objectives defined and based upon risk to state entities
- Aligned to “Framework for Improving Critical Infrastructure Cybersecurity” released by NIST in February 2014
- Objectives to expand over time

CISO Updates

Security Terms & Conditions

- **Ensuring minimum security safeguards**
 - NIST 800-53 vs. ISO 27001
 - Security breach procedures
 - Control for disclosure of breaches to third parties
 - Oversight of security compliance
 - Return of destruction of personal information
 - FedRAMP system requirements
 - Indemnification



Introducing...

Barbara Garrett

**Deputy Director,
Statewide Telecommunication &
Network Division**



California
DEPARTMENT OF TECHNOLOGY

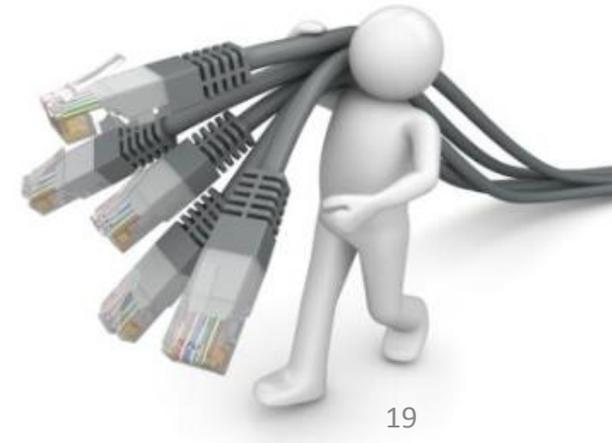
CALNET 2

Structured Cabling:

- No new orders allowed after January 29, 2017
- Orders must be completed and invoiced by January 28, 2018
- Like services now available on MiCTA

Equipment:

- Orders must be fulfilled and invoiced by January 28, 2018



CALNET 3

Category 10: Satellite contracts awarded

- 10.1: Satellite Voice – 4 Vendors
- 10.2: Satellite Data – 2 Vendors

Refresh:

- Category 3: Metropolitan Area Network – Ethernet
- Category 5: Managed Internet
- Awards for both targeted for December 2016

Category 14:

- Broadband Internet pre-solicitation release targeted for early November 2016

Category 1.6:

- Extending 1 year through June 2018





Presenters' Contact Information

Chris Cruz: Chris.Cruz@state.ca.gov

Jim Butler: Jim.Butler@dgs.ca.gov

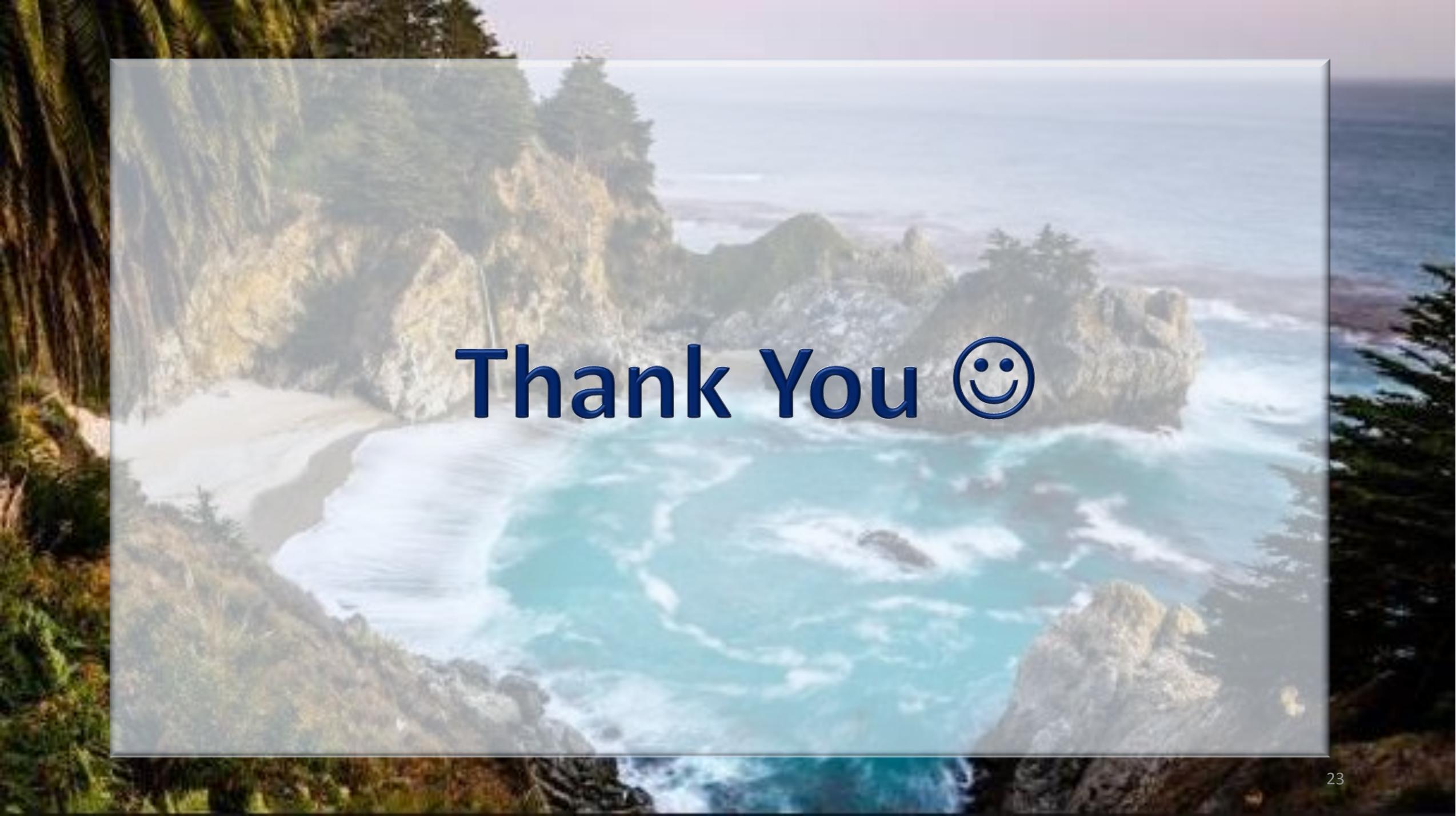
Scott MacDonald: Scott.MacDonald@state.ca.gov

Richard Rogers: Richard.Rogers@state.ca.gov

David Langston: David.Langston@state.ca.gov

Barbara Garrett: Barbara.Garrett@state.ca.gov

contact us



Thank You 😊