RESEARCH ADVISORY BOARD (RAB)  
October 6, 2015  
8-9:30am  
Medical Sciences Building, Chancellors Conference Room S-30

Attendees: Chip Chambers, Jane Czech, Clarice Estrada, John Jones, Jean Jones, Mounira Kenaani, Jim Kiriakis, Gretchen Kiser, Georgina Lopez, Wallace Marshall, Suzanne Murphy, Michael Nordberg, Marge O’Halloran, Anja Paardekooper, Bill Seaman, Brian Smith, Matt Springer, Paul Volberding  
Not here: MC Gaisbauer, Jennifer Grandis, Larisa Kure, Irene McGlynn, Synthia Mellon, Teresa Moeller, Thomas Neylan, Christine Razler, Nirao Shah  
On Phone: Vanessa Jacoby, Terri O’Lornergan  
Guests: Pat Phelan, Eunice Stephens, Bruce Wintroub, Karin Wong

PRESENTATION: Space Discussion, Bruce Wintroub and Karin Wong

Bruce Wintroub and Karin Wong gave an update on space at UCSF (see PowerPoint presentation)

- Major change: Space assignments do not indicate ownership and are not permanent. Schools are the fiduciaries of the Chancellor; space is controlled by the Chancellor and is assigned to Schools to be allocated and used appropriately and effectively.
- Modernization of Parnassus: some feel that it is the forgotten campus, but that is not the case. We are limited in not being able to build any new buildings, but there are a number of changes/renovations happening, including the renovation of the Clinical Sciences Building, UC Hall, and multiple floors of the HSIR towers and Medical Sciences Buildings.
  - Not all of the money is going to Mission Bay! Over the next 7 years, UCSF will invest approximately $400 into the beginning of the modernization of Parnassus.
- Mission Bay
  - Block 33 will house academic and administrative office space, clinical space and other necessary support for various units currently distributed at multiple UCSF sites, including Laurel Heights. This building should be occupied by 2019 and Laurel Heights should be largely empty.
    - Laurel Heights has been leased, with a 99 year lease, we will need to vacate within 5 years. There will be space for everyone from that campus at either Mission Bay, Mt. Zion or Parnassus
  - Precision Cancer Building is to grow outpatient clinical programs in Cancer, Psychiatry, Ophthalmology and primary/secondary care. Hope to move in by late 2018
  - Proposed Block 23A Building for Neurosciences research laboratory building including clinics, dry and wet labs and a vivarium.
- SFGH
  - San Francisco General Hospital Research Building for Bench lab research, desktop research and office space
    - House approximately 800 existing UCSF employees at SFGH

Questions/Comments:

- Lessons to be learned from Mission Hall, which should be considered before people move in the various new buildings. Would recommend having a written understanding and buy-in from all interested parties
  - Working with Michael Bade on this issue, what can be expected, what should be budgeted for, etc.
- Parnassus: For the non-renovated areas, how can the people there be involved in this discussion?
  - Contact your appropriate Department Chair, who can then share comprehensive feedback to the Dean’s. The EVCP Office will share more information as it becomes available of long-term modernization of Parnassus., We want people to know this is happening and have buy-in and be part of the process so that what is done
- Mission Bay: Is there any discussion with donors to put some funding into endowments for future maintenance?
  - This is a tough issue, things are still jelling
- Mission Bay: what will happen with the Warriors stadium and our new buildings going in, in terms of parking and traffic
  - Campus planning and Chancellors office are working on this. A UCSF Warriors Working Group meets regularly with Warriors and has representation from many UCSF departments including Parking & Transportation who will address concerns about parking and transportation around the Mission Bay campus.
- There is a lot of work being done with Mission Hall to have things work better.

Next Steps:
None noted

PRESENTATION: IT Security Update, Pat Phelan
Pat Phelan gave an update on the IT Security Update (see PowerPoint presentation)
• UCSF has been anxious about IT security for a number of years, and with what happened at UCLA, UCSF has become more aggressive re IT security, with the encouragement of UCOP and the President’s office
  o UCSF Roadmap
    • Since 2014, UCSF has launched numerous security initiatives, spurred by several drivers:
      • Enterprise risk assessment identified compliance gaps
      • Scrutiny from federal and state regulators due to past incidents
      • Increase in volume and severity of threats
      • Increased investment in security initiatives begin in 2014; additional funding secured in August to kick start activities
      • Recent activity was already on the three-year roadmap, but timelines have been shortened
• UC President Janet Napolitano has mandated appointment of an executive to report cybersecurity risks and remediation to the Chancellor at each Campus
  o Joe Bengfort is UCSF’s representative
• There will be security training required of all faculty, staff and trainees
• Asset management/BigFix
  o Knowing what devices are on the network, their patch status, and to whom they belong is critical to protecting UCSF data and computing resources and to satisfy compliance requirements.
  o BigFix allows IT to track an asset, associate a computer to a person, and collect system information.
  o Unidentified, unregistered devices on the UCSF network are a risk to every other device on the UCSF network and will be subject to removal from the UCSF network after August 14, 2015.
• IT is currently scanning the entire system for vulnerabilities
  o If IT cannot identify a device and it doesn’t have BigFix installed, the account/device will be deactivated
    • At this point, approximately 5 have been removed

Questions/Comments:
• For security training
  o If there is push back, it is appropriate to let people know that UCSF pushed back on UCOP on what the training would look like and rollout timing, and were told we needed to move forward.
  o Could also do in-person trainings to cover people that do not have regular computer access/use

Next Steps:
• Pat, Georgina, Matt meet to discuss changes to VPN
Research Advisory Board (RAB)

UCSF Space Update

Bruce Wintroub, MD
Chair of Dermatology and Vice Dean
UCSF School of Medicine

10/6/2015
UCSF Parnassus campus
Modernization of Parnassus

Clinical Sciences Building
- Post renovation will be office and instructional space
- First Floor: Instructional space
- Floors 2-7: open space design
- Budget: $95M
- 109,126 gsf
- Timeline
  - May 2013: Preliminary funding approval
  - Jul-Nov 2013: Faculty Advisory Committee Meetings
  - Dec 2013-Jul 2014: Interior Improvement Design
  - Jan 2016-Dec 2017: Construction
  - Jan 2018: Anticipated Occupancy
Modernization of Parnassus

Clinical Sciences Building Workstation Supply/Demand

<table>
<thead>
<tr>
<th>Supply</th>
<th>Demand</th>
<th>Remaining Supply</th>
<th>Additional Demand</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>498</td>
<td>446</td>
<td>52</td>
<td>65</td>
<td>-13</td>
</tr>
</tbody>
</table>

Illustration of Private Office and Workstation Supply on Floors 2-7

<table>
<thead>
<tr>
<th>Private Office Supply</th>
<th>Workstation Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>169</td>
<td>304</td>
</tr>
</tbody>
</table>
Modernization of Parnassus

Clinical Sciences Building: Saunders Court entrance
Modernization of Parnassus

Level 1
Modernization of Parnassus

Level 3 (Typical for levels 2 - 5)
Modernization of Parnassus

Projected 7 year investment in Parnassus capital improvements
Approximately $400M

• U80: Completed and occupied
• HSE 8 and HSE7A: Completed and occupied
• HSE 608: Completed and occupied
• HSW8: Completed and occupied
• HSW7: Completed and occupied
• HSE7B: scheduled completion October 2015
• Medical Sciences 2-6: Demo/construction began May 2015
• Medical Sciences 7 & 8: Demo/construction began June 2015
• LabRad Demo: January 2016 completion
• MR4 Demo: May 2016 completion
• Utilities Relocation Phase 1: January 2016 completion
UCSF Mission Bay Campus
Block 33 Building

- Mission Bay East Campus Phase I Building: Block 33
  - Academic and administrative office space, clinical space and other necessary support for various units currently distributed at multiple UCSF sites, including Laurel Heights.
  - Preliminary funding plans $237.1M from campus funds, external financing, medical center funds and gift funds.
  - Located on corner of Third and 16th Street, adjacent to Gateway Building
  - 340,000 gsf

Project Location: Block 33 Building
Precision Cancer Building

- Clinical strategy to grow outpatient clinical programs in Cancer, Psychiatry, Ophthalmology and primary/secondary care
- Preliminary funding plans $16.6M
- Located on corner of Third and 16th Street, adjacent to Gateway Building
- 170,000 gsf
- Following all approvals, estimate timeline early 2017 – late 2018
Proposed Block 23A Building

- Neurosciences research laboratory building including clinics, dry and wet labs and a vivarium
- Approximately 275,000 gsf
- Expected Regents approval in mid-2016
San Francisco General Hospital (SFGH)
San Francisco General Hospital Research Building

- 175,000 gsf
- Bench lab research, desktop research and office space
- House approximately 800 existing UCSF employees at SFGH
- Initial project budget limit established at $188M, which will be financed by UCSF
- Lease terms – 75 years, plus 24-year option
- Timeline:
  - Programming Sep 2015-Jan 2016
  - Design Jun 2016 – June 2017
  - Build 2017 – 2019
Proposed Research Building Location
UCSF IT Security Acceleration
Research Advisory Board

Joe Bengfort, Chief Information Officer
Patrick Phelan, Information Security Officer

10/5/2015
UCSF Security Roadmap

Since 2014, UCSF has launched numerous security initiatives, spurred by several drivers:

- Enterprise risk assessment identified compliance gaps
- Scrutiny from federal and state regulators due to past incidents
- Increase in volume and severity of threats

Increased investment in security initiatives begin in 2014; additional funding secured in August to kick start activities

Recent activity was already on the three-year roadmap, but timelines have been shortened
Why the Acceleration of IT Security

- We are taking steps to better secure our systems as part of our ongoing effort to strengthen network security at UCSF, and in light of recent attacks on higher education and research institutions.

- Demonstrate to our patients, regulators, and legislators that UC and UCSF respects patient privacy by aggressively implementing stronger security controls.

- Safeguard PHI, intellectual property, and PII by preventing unauthorized computers from connecting to the UCSF network.

- Janet Napolitano has mandated appointment of an executive to report cybersecurity risks and remediation to the Chancellor at each Campus
## UCSF Accelerated IT Security Program

<table>
<thead>
<tr>
<th>Action</th>
<th>Value</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin. Password Changes</td>
<td>Decrease likelihood of hackers gaining access</td>
<td>Complete</td>
</tr>
<tr>
<td>System patching</td>
<td>Addresses most common entry point for hackers</td>
<td>Complete/ongoing</td>
</tr>
<tr>
<td>System Scanning</td>
<td>Identifies vulnerabilities and remediation actions.</td>
<td>Complete/ongoing</td>
</tr>
<tr>
<td>BigFix Deployment</td>
<td>Provides visibility and degree of control.</td>
<td>75% Complete</td>
</tr>
<tr>
<td>Firewall Hardening</td>
<td>Blocks malicious traffic of known types</td>
<td>Complete</td>
</tr>
<tr>
<td>VPN Consolidation</td>
<td>Reduced number of access methods</td>
<td>Complete</td>
</tr>
<tr>
<td>Two-factor Authentication</td>
<td>Prevent hackers’ use of stolen credentials</td>
<td>Complete</td>
</tr>
</tbody>
</table>

Note: Accelerated plan runs August – October 2015
UC Cyber-Risk Responsible Executive

• Authority to direct cybersecurity resources in any part of the campus enterprise.

• Responsible to develop cybersecurity risk mgmt.
  – 120-day plan to accelerate risk mitigation
  – 3-year cyber-risk management strategy

• UCOP provided security training for all faculty, staff, trainees.

• Develop cybersecurity resource plan and implementation timeline
Border firewall

- The overwhelming majority of inbound traffic from the Internet is malicious; UCSF has traditionally allowed all inbound traffic.

- UCSF began systematically blocking unwanted traffic in Fall 2014, collecting exceptions from system owners.

- The initiative was scheduled to be completed in December 2015, but accelerated to July 30.

- [https://secureborder.ucsf.edu](https://secureborder.ucsf.edu)
Patching

Unpatched computers are the most frequently used entrance point for malicious activity. Any vulnerable computer may be used to attack others on the UCSF network.

• Security patching of all desktops and laptops with BigFix installed began July 23. Prior to that, only ITFS managed desktops and laptops were patched using BigFix.

• All BigFix desktops and laptops will be patched monthly going forward.

• Accelerated patching of IT managed servers began July 23. The regular server patching cycle has been shortened from quarterly to monthly.
Vulnerability scanning

• We use Tenable SecurityCenter:
  – To identify vulnerable, misconfigured, or compromised hosts
  – To help system administrators validate proper configuration and patching of their systems
  – To prioritize addressing the highest risk systems first

• Until now, vulnerability scans have focused on either specific systems or specific vulnerabilities rather than the network at large.

• Comprehensive scans including the entire UCSF network began at the end of July and are now roughly monthly.

• Authenticated scanning results in faster, more accurate scan results with fewer issues.
Privileged account passwords

- Strong, regularly changed passwords are an effective safeguard against automated attack tools
- Local administrator passwords have been changed on managed systems and will be changed regularly (monthly in the case of managed desktops)
- UCSF IT is using a 15-character, 90-day maximum age standard for privileged/administrator accounts
- The UCSF Minimum Security Standards updated to require the above standard on Windows machines:
  - “Privileged administrator accounts with access to sensitive Windows systems should use passphrases that are 15 or more characters in length and meet the Unified UCSF Enterprise Password Standard. Passphrases should be reset at least every 90 days.”
DUO two-factor authentication

Why DUO

- Two factor authentication requires a second factor to complete the login process and is extremely
- DUO on VPN prevents someone with stolen credentials from remotely accessing our network
- DUO on servers prevents someone with stolen credentials from logging on to our machines

Status

- Remote access via VPN for privileged users
  - Required and in-place for UCSF IT
  - Being rolled out to departmental IT administrators; near-term future requirement
- Access to servers by privileged users
  - Rolled out to UCSF IT servers
  - UCSF IT plans to offer this to departmental IT administrators

More information

- [http://it.ucsf.edu/projects/duo-two-factor-authentication](http://it.ucsf.edu/projects/duo-two-factor-authentication)
Asset management/BigFix

- Having visibility into what devices are on the network, their patch status, and to whom they belong is critical to protecting UCSF data and computing resources and to satisfy compliance requirements.

- BigFix allows IT to track an asset, associate a computer to a person, and collect system information.

- Unidentified, unregistered devices on the UCSF network are a risk to every other device on the UCSF network and will be subject to removal from the UCSF network after August 14, 2015.
Registration: Immediate Action Required

As of August 17, 2015, all laptops and desktops used for UCSF business (UCSF owned or personally owned) must be registered by installing BigFix*.

1. To verify that BigFix is installed on your computer look for this icon on your laptop or desktop. 

2. If BigFix is already installed, your registration is complete; no further action required.

3. If you don’t see the BigFix icon, install BigFix by going here: http://it.ucsf.edu/services/bigfix-endpoint-manager

4. If you need assistance or have questions, please contact the IT Service Desk at 415-514-4100.

5. BigFix Frequently Asked Questions: http://tiny.ucsf.edu/bffaq
Taking Control of the Network

- Establish the network as:
  - UCSF enterprise asset;
  - That the CIO is accountable to manage and protect;
  - That requires minimum standards to access;
  - As a privilege and not a right.

- Actions that this drives:
  - Requires a complete inventory (registration) of what is attached to the network.
  - Installing BigFix is the primary registration method.
  - Manual registration for any devices that cannot run BigFix for technical or material business reasons.
  - Remove at-risk devices from the network that are not registered in a timely manner.
What Happens to Unregistered Devices?

Any devices that have not installed BigFix, or registered manually are considered a risk to UCSF, and are subject to removal from the UCSF network. In an effort to mitigate impact to UCSF business:

- UCSF IT will not disconnect computers where specific issues have been identified and you are collaborating with UCSF IT to resolve.

- UCSF IT will incrementally remove high-risk computers from the UCSF network that have not been registered.

- Departmental IT teams will be notified of computers scheduled for removal from the UCSF network 3 business days prior to disconnection. Ask your departmental IT team members to subscribe to the IT-Forum mailing list.
  - Subscribe to the IT-Forum mailing list by sending an email to listserv@listsrv.ucsf.edu with a blank subject line; in the body of the email message include: Subscribe IT-Forum

- An expedited process is in place to assist in remediating and returning network connectivity by contacting the IT Service Desk at 415-514-4100.
Email to Require VPN

- Currently, you can use email clients like Outlook, Mac Mail, and Eudora from anywhere in the world. Most organizations do not allow this.

- This can result in machines downloading sensitive information without being subject to UCSF’s security controls.

- Beginning October 20\textsuperscript{th}, 2015, you will be required to use VPN to access your email.

- This does \textbf{not} affect smartphones, tablets, or Outlook Web Access (https://mail.ucsf.edu)