SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

August 9, 2013

MICHAEL L. NORMAN
Director
San Diego Supercomputer Center
0505

Subject: ***Information Technology Security – San Diego Supercomputer Center (SDSC) Audit & Management Advisory Services Project 2013-03***

The final audit report for Information Technology Security – San Diego Supercomputer Center, Audit Report 2013-03, is attached. We would like to thank all members of SDSC for their cooperation and assistance throughout the review.

We have reached agreement with SDSC management for corrective actions to be taken for issues noted during our review, and these corrective actions are noted in this final report. Therefore, we do not request a formal response to the report. The corrective actions will be added to our follow-up system, and we will contact SDSC management to initiate a follow-up review of these actions at the appropriate.

UC wide policy requires that all draft audit reports, both printed and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to us or destroy them at this time. Thank you.

David Meier
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: W. Armstrong
S. Brown
M. Campbell
C. Klock
D. Larson
G. Matthews
R. Moore
A. Palazzolo
S. Subramani
S. Vacca

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Information Technology Security – San Diego Supercomputer Center
June 2013

Performed By:

Greg Buchanan, Auditor
Daren Kinser, Auditor

Approved By:

David Meier, Assistant Vice Chancellor

Project Number: 2013-03

Information Technology Security – San Diego Supercomputer Center
Audit & Management Advisory Services Project 2013-03

Table of Contents

I. Background 1
II. Audit Objective, Scope, and Procedures 2
III. Conclusion 3
IV. Observations and Management Corrective Actions 3
A. Data Center Access Controls 3
B. VM Compliance SLA 6
C. Colocation SLA 7
D. Colocation Vulnerability Scanning 8

ATTACHMENT A – SDSC Systems and Services Overview

Information Technology Security – San Diego Supercomputer Center
Audit & Management Advisory Services Project 2013-03

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of Information Technology Security at the San Diego Supercomputer Center (SDSC) as part of the approved audit plan for Fiscal Year 2012-03. This report summarizes the results of our review.

SDSC is an Organized Research Unit of UCSD whose mission is to transform science and society at UC San Diego and across the nation through world-leading cyber-infrastructure innovation, development, and expertise. In recent years, SDSC has focused on developing cyber-infrastructure services dedicated to research endeavors that involved extremely large data sets, oftentimes referred to as "Big Data." In 2012 SDSC introduced Gordon, a high-performance computing (HPC) resource that uses massive amounts of flash-based memory. Gordon, along with other HPC resources such as Trestles and Triton, are utilized by approximately 1,600 researchers including 150 principal investigators across eight UC campuses to conduct data-intensive research, analysis and high-end virtualization. Projects span a range of scientific disciplines, including: gene sequencing; conceptualization of nanoparticles; modeling the impact of climate change; and others.

In addition to high performance computing and data intensive research endeavors, SDSC offers a wide array of recharge-based services to UCSD researchers and departments, the broader UC community, and to some external industry partners. These services include Data Center colocation, data storage, IT systems support, virtual machine (VM) services, networking services, and compute cycles. Some of these services, such as colocation and data storage, are offered to UCSD researchers at subsidized rates through the UCSD Research Cyberinfrastructure (RCI).

The largest and most utilized service offering is SDSC Data Center colocation[1], which averages approximately $1.8 million in recharges annually. The colocation services provides campus-wide opportunities to realize energy efficiency, reduce capital and operating costs, and ultimately increase the competitiveness and capabilities of the University. Colocation devices are housed within the SDSC's 19,000 Data Center, and leverage the center's robust physical and environmental controls.

The sensitivity of the data and systems housed at SDSC varies from system to system, and responsibility for securing the data and systems is somewhat decentralized. **Attachment A** provides a high level overview of the various SDSC systems and services, including the sensitivity of data and responsibility for IT security, depending on the nature of the system or service being provided. The most sensitive systems are supported by the SDSC Health Cyberinfrastructure. In August 2009, SDSC was subcontracted by the Chickasaw Nation Industries to operate and maintain the Center for Medicare and

[1] Colocation refers to the provisioning of computing services in a third party center.

Medical Services (CMS) Medicare Integrity Group (MIG) Data Engine, which is classified as a Federal Information Security Management Act (FISMA) moderate risk system. In accordance with the subcontract, one third of the systems security requirements are internally audited by SDSC Health Cyberinfrastructure staff on an annual basis, and all controls are audited by an external agency once every three years.

II. Audit Objective, Scope, and Procedures

The objective of our review was to determine if the SDSC IT security practices were adequate to ensure that contractual requirements relating to the confidentiality, integrity and availability of data and systems housed within the SDSC Data Center were being fulfilled, and that highly sensitive systems were being managed in compliance with applicable regulatory requirements.

In order to achieve our objectives we completed the following:

- Interviewed the following SDSC personnel:
  - Deputy Director,
  - Chief Information Security Officer (CISO),
  - Business Services Officer,
  - Data Center Manager,
  - Health Cyberinfrastructure Division Director,
  - IT Systems and Services (ITSS) Division Director,
  - ITSS Storage Systems Manager, and
  - ITSS Microsoft and Visualized Platforms Manager;
- Reviewed technical specifications for the Data Center, the SDSC Cloud Storage environment, and SDSC Project Storage environment;
- Reviewed the National Institutes of Standards and Technology (NIST) Special Publication 800-53;
- Reviewed the MIG Data Engine Operations and Maintenance contract proposal dated August 7, 2009;
- Reviewed the 2011 MIG Data Engine external audit report, the 2012 MIG Data Engine internal audit, and the May 9, 2013 nCircle vulnerability scan of the MIG Data Engine environment;
- Conducted a tour of the SDSC Data Center, and evaluated physical and environmental controls against NIST Special Publication 800-53 low risk security requirements;
- Reviewed and evaluated the boilerplate Cloud Services Service Agreement, the UC Davis VM Compliance Service Level Agreement (SLA), and 30 randomly selected colocation SLAs and service agreements;
- Reviewed SDSC Nessus Vulnerability Scan reports for two of the colocation devices that SDSC is responsible for patching and updating; and

- Evaluated the VM Compliance environment's compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule sections 164.310.d.2.ii, 164.312.b and 164.316.b.i.

III. Conclusion

We concluded that SDSC IT security practices were generally adequate to ensure that contractual requirements relating to the confidentiality, integrity and availability of data and systems housed within the SDSC Data Center were being fulfilled, and that highly sensitive systems were being managed in compliance with applicable regulatory requirements.

However, we did identify ways in which SDSC could improve access controls at the Data Center. We also identified ways that the SLA language for the VM Compliance and Colocation services could be improved in order to clarify customer responsibilities in regards to logical security. Further, SDSC Nessus vulnerability scans could be more effectively used to evaluate patching levels over all colocation devices that are patched and updated by SDSC personnel. These findings are discussed in further detail in the balance of this report.

IV. Observations and Management Corrective Actions

A. Data Center Access Controls

The SDSC Data Center could improve access controls to ensure timely termination of access credentials for individuals who are transferred or separated. Further, the Data Center could improve security over colocation devices by installing mantraps or rotating security doors at the main Data Center entrance, and by locking racks that are found to be unlocked and unattended.

Because the Data Center is utilized by a significant number of UCSD departments, as well as other UC campuses and external customers, it is important that the Data Center implement adequate logical and physical access controls to ensure that only authorized individuals access equipment in the facility. Access controls include the provisioning and de-provisioning of accounts and credentials, and ensuring that credentials are terminated when individuals are transferred or separated. Access controls also include limiting access to the facility and equipment using physical safeguards, and verifying individual credentials before providing access to the facility and equipment.

Termination of Access Credentials

In general, the Data Center implemented strong access controls. Access to the facility was controlled via a unique access code and biometric scanner, and the Data Center verified individuals prior to providing them with credentials.

SDSC has implemented a check-out process which ensures that Data Center access is terminated when SDSC personnel are separated or transfer to another department. However, the Data Center did not have a process in place to ensure that access credentials were terminated in a timely manner when non-SDSC individuals were transferred or separated. The Data Center terminated access only when notified by the colocation customer that an authorized individual was transferred or separated, or when Data Center personnel learned anecdotally that an authorized individual no longer was employed by the colocation customer. Further, access credentials were configured to never expire. As a result, there was significant risk that individuals could continue to access the Data Center for a significant amount of time after transferring or separating from the colocation customer.

Management Corrective Actions:

SDSD will implement a check-out process to ensure that Data Center access is terminated in a timely manner when non-SDSC personnel are separated or transferred. Options that SDSC will consider include working with Human Resources to regularly obtain and review a listing of UCSD personnel actions, and/or configuring Data Center credentials to expire.

Unauthorized Access/Piggybacking

Piggybacking is a term used to describe instances in which an authorized individual unlocks and enters a security door and allows another individual to follow them in, and is a method used by intruders to access restricted facilities, such as the Data Center. Piggybacking is prevented by installing revolving security doors or mantraps. A mantrap is a mechanism involving two doors, where the first door must be fully closed before opening the second door, and vise-versa. A revolving security door is a turnstile type device that allows only one person through at a time.

Access to the Data Center was restricted using a single door that could be opened by entering an access code and providing a biometric hand scan. This configuration was not sufficient to prevent piggybacking. Because the Data Center is staffed at all times, the risk of piggybacking may be mitigated by SDSC

personnel correcting the behavior. However, Data Center personnel indicated that there have been numerous instances in which individuals have opened the security door and held it open for another individual that did not provide access credentials.

The Data Center had obtained estimates for the installation of a mantrap and a revolving security door, but a formal decision to install a solution had not yet made made.

Management Corrective Action:

SDSC will continue to evaluate the cost-benefit of installing a mantrap or revolving door, or other mitigating controls, which would improve physical access controls.

Unlocked Racks

Many of the colocation customers have purchased locking racks to enhance physical security over their devices within the Data Center. Locking racks are required for customers that house sensitive data, and optional for all other customers.

Data Center personnel perform regular walkthroughs of the Data Center, during which personnel sometimes encounter racks that are unlocked and unattended. However, due to uncertainty as to whether or not locking customer racks is within the responsibilities of Data Center personnel, Data Center management had not yet directed personnel to lock unattended racks. One of the primary reasons was that the Data Center did not wish to take responsibility for locking a rack when a customer or third party vendor had temporarily stepped away from device. However, taking no action may result in a racked being left unlocked for a significant amount of time, thereby increasing the risk that the device could be compromised.

Management Corrective Action:

The Data Center will develop a policy for ensuring that designated racks are locked.

B. VM Compliance SLA

SLA language for the VM Compliance environment could be improved to clarify customer responsibilities in regards to logical security.

Depending on the security needs of the customer, the SDSC ITSS group offered two different VM services: a standard VM service and a VM Compliance service. The VM Compliance service was developed by the SDSC ITSS group to provide a VM environment that could be used by customers handling ePHI to ensure compliance with HIPAA[2] regulations. As such, the VM Compliance environment had additional logical security features in place such as a hardware firewall and hard disk encryption.

As of the date of this review, there were only four VM Compliance customers, two of which were UCSD departments, and two of which were other UC campuses. SDSC ITSS had not yet determined whether or not the VM Compliance service would be offered to non-UCSD customers. The SDSC ITSS offered to provide each customer with additional services to guarantee full HIPAA compliance over their VM environment, at an additional cost. All customers declined these additional services. As such, the SLA's Scope of Work statement was updated to include the following language:

> *It is the Customer's responsibility to determine whether the Customer's environment within SDSC's VM Services meets all applicable laws and government regulations, including HIPAA regulations, if applicable. SDSC has offered to provide security and compliance assessments (for a fee), to Customer while maintaining sole administrative access to the customer servers. These services have been declined and Customer has chosen to perform these security services in-house. Due to the fact that SDSC does not have sole administrative privileges for Customer's data, SDSC cannot guarantee that Customer's environment will be suitable to house data that falls within HIPAA compliancy regulations. As such, Customer and SDSC agree that SDSC will not be liable for any breach of data within hosted environment.*

Because all VM Compliance customers were internal to UC, it is in the best interest of SDSC to ensure that their VM Compliance customers fully understand the scope of the security services being provided within the environment so that they can ensure that those controls, combined with security controls that they implement, are in compliance with applicable laws and regulations. While the SLA cited above clearly indicates that the customer is responsible for ensuring compliance with HIPAA or other regulatory requirements, the SLA did not

[2] Health Insurance Portability and Accountability Act of 1996

provide detail on the scope and nature of the security services provided by SDSC within the environment.

In consultation with the ITSS personnel that manage the VM Compliance environment, the SDSC CISO drafted an internal HIPAA Compliance Policy outlining the security features that have been implemented by SDSC within the VM Compliance environment to help ensure that customers can maintain a HIPAA compliant environment. Once finalized, this policy could be used to update the VM Compliance SLA so that it includes specific security features being provided within the environment.

Management Corrective Actions:

SDSC will modify the draft internal HIPAA Compliance Policy, and update the VM Compliance SLA to include the security features that are detailed in the policy. Further, SDSC will work with Procurement & Contracts and Campus Counsel to develop service agreement language for non-UC customers.

C. Colocation SLA

The Colocation SLA could be improved by including an explicit statement that the customers are responsible for implementing logical security over their colocation devices, and are responsible for ensuring compliance with the UCSD Minimum Network Connection Standards and UC Policy IS-3.

Personnel who administer devices that are connected to the UCSD Campus network are required to follow UCSD Policy and Procedure Manual 135-3, Exhibit B – UCSD Minimum Network Connection Standards. These standards set forth various requirements for logical and physical security based on the sensitivity and use of the device. In addition, all UC personnel are required to follow UCOP Policy IS-3, Electronic Information Security, which requires personnel to complete a risk assessment of their data and systems, and implement appropriate physical and logical security controls based on the risk level of their systems and data.

SDSC has utilized several versions of the SLA template to enter into colocation agreements with customers since initiating the service in 2008. Based on our review of 30 randomly selected colocation agreements, it appears that prior to January 2011 all colocation SLAs entered into with UCSD customers included a listing of customer duties, one of which was compliance with the UCSD minimum security standards. In January 2011, SDSC removed all references to the UCSD minimum network security standards from the SLA.

The most recent version of the SLA (the SDSC ITSS and Colocation Core Service Level Agreement) reflects a cafeteria style approach to offering SDSC services to internal customers. The Core SLA is used for all internal customers regardless of the services the customers wish to purchase. SDSC then attaches standardized exhibits to reflect the specific nature and scope of the services being provided by SDSC, including Exhibit J which is used for SDSC Colocation Services.

The SDSC ITSS and Colocation Core Service Level Agreement contains a data security section (section 6.4) that states "Customers and End Users are responsible for the security of their data and are required to protect his or her password(s)." However, this data security section is somewhat confusing and appears to apply more to SDSC Cloud services. In addition, Exhibit J contains no statement on customer responsibilities in regards to data or system security and for ensuring compliance with the UCSD Minimum Network Connection Standards and UCOP Policy IS-3. As a result, some colocation customers could misinterpret their responsibilities in regards to logical security and compliance with applicable policies.

Management Corrective Action:

The SDSC ITSS and Colocation Core Service Level Agreement, Exhibit J will be updated to more explicitly indicate that UCSD customers are responsible for ensuring compliance with UCSD Minimum Network Connection Standards and all UCOP policies pertaining to IS security, unless the customer has opted to purchase logical security and system administration services from SDSC.

D. Colocation Vulnerability Scanning

SDSC Nessus vulnerability scans could be used more effectively to evaluate patching levels over all colocation devices that are maintained by SDSC personnel.

As a best practice, system administrators can use vulnerability scanning tools to verify that their systems are adequately patched, and that the systems do not contain any critical or high risk vulnerabilities. At UCSD, Administrative Computing and Telecommunications (ACT) provides a service for system administrators to run their own vulnerability scans using the Qualys Vulnerability Management system. Alternatively, system administrators could acquire their own vulnerability scanners and scan systems that they are responsible for patching and updating.

Colocation devices are placed in one of two different internet protocol (IP) address spaces. Non-UCSD devices are placed in SDSC IP address space, which is not part of the Campus network, and UCSD customer devices are placed in Campus IP address space. The SDSC CISO uses a Nessus Vulnerability Scanner to regularly scan devices the SDSC IP address space in order to identify machines that contain significant vulnerabilities or have possibly been compromised. However, because the Campus IP address space was being regularly scanned using Qualys, ACT advised SDSC not to run Nessus scans on colocation devices residing in Campus IP address space.

A number of UCSD and non-UCSD colocation customers have contracted with SDSC ITSS to provide system support, including patching and updating. While SDSC system administrators responsible for providing these services regularly received and reviewed Nessus Vulnerability Scanner results, these results did not include supported systems that resided in the Campus IP address space. Therefore, SDSC systems administrators were unable to fully assess these systems for weaknesses.

During our review, we were advised by ACT that although they do generally prohibit SDSC from scanning the Campus IP address space, it is acceptable to run vulnerability scans on systems on which they retain administrative rights.

Management Corrective Actions:

SDSC will expand the regular Nessus Vulnerability Scans to include SDSC supported colocation devices that reside in Campus IP address space, and provide the scan results to the responsible systems administrator so that they can fully evaluate the systems for weaknesses.

Information Technology Security – San Diego Supercomputer Center
Audit & Management Advisory Services Project 2013-03

				Research CyberInfrastructure (RCI)		IT Systems and Services (D)			
	SDSC Research Devices	SDSC Business Services (E)	Health CyberInfrastructure (MIG Data Engine)	Co-Location (C)	Triton Shared Compute Cluster	Co-Location	Storage (Cloud and Project)	CommVault	VM Services
Attributes									
Users	UC Researchers and National Users (XSEDE)	SDSC Business Users, some UC Administrators and Researchers	CMS Contractors	UC Researchers		UCSD/UC Campuses/External Customers			
Funding	Extramural Funding/Systemwide Funding	Departmental/ Extramural Funding/ Some Recharge	Extramural Funding	Campus Subsidies/Extramural Funds/Department Funds		Departmental and External Recharges			
Campus Oversight Body	N/A	N/A	N/A	RCI Oversight Committee		N/A			
Sensitivity of Data (Type)	Varies - Research Devices	Low (No PII, PCI, ePHI)	High (ePHI)	Varies Per Customer	Varies by customer (no EAR/ITAR/ ePHI/PII)	Varies Per Customer	None**(A)**	Varies Per Customer	Varies Per Customer **(B)**
Management of Physical Security	Data Center Personnel	Data Center Personnel	Data Center Personnel	Data Center Personnel	Data Center Personnel	Data Center Personnel			
Management of Logical Security	PI Responsibility	SDSC Business Services in coordination with IT Systems and Services Personnel	SDSC Chief Information Security Officer	Varies based on MOU	SDSC Technical Personnel	Varies based on MOU/SA	SDSC IT Systems and Services Personnel	SDSC IT Systems and Services Personnel	SDSC IT Systems and Services Personnel

Footnotes:

(A) Cloud users are generally prohibited from storing unencryted sensitive personal identify information and ePHI. Export controls are strictly prohibited.

(B) VM Services maintain two environments: the standard environment and the compliance. The standard environment is managed similar to cloud computing in that unencrypted sensitive data (PII/ePHI) is prohibited, and export controls are strictly prohibited. The compliance environment does not restrict the storage of ePHI.

(C) RCI Co-Location includes locations at Cal-IT2 (Qualcomm Institute), Scripps Insititution of Oceanography (SIO) and Academic Computing and Media Services (ACMS). SDSC is only responsible for physical security over the SDSC data center co-location.

(D) In addition to the services documented in the chart, IT Systems and Services also offers enterprise networking services, and IT services for Unix and Sun-based systems inside and outside of the data center.

(E) SDSC's WEB/DB recharge activities are operated within SDSC Business Services and customers are generally hosting nonsensitive data. Customers who requests to host sensitive (e.g., HIPAA data) are referred to the IT Systems group for a secure solution.