Rutgers University Senate
Research and Graduate & Professional Education Committee (RGPEC)
Report and Recommendations on Research Support Infrastructure

The Charge

On September 7, 2012, the Senate Research and Graduate & Professional Education Committee (RGPEC) was charged as follows:

> *In preparation for the Rutgers/UMD merger, investigate the status of the research support infrastructure at Rutgers, including instrumentation, equipment, maintenance contracts, site licenses, and shared data storage. Provide recommendations that have the potential to reduce associated costs and enhance opportunities for information, equipment, and instrumentation sharing. Provide recommendations about research data security and academic and non-academic support services.*

To address the complexity of the charge, the committee created five subcharges looking at different aspects of research infrastructure:

S-1108.1   **Data and Information Sharing**: Public vs. private; RUcore access; Seminars/workshops; Streaming video, video on demand

S-1108.2   **Secure Data Storage**: Data storage; Local, central, cloud; Access; Working data vs. archived data; Costs; Federal policies re data access and storage

S-1108.3   **Data Transport**: Data transport; Networking; Internet2

S-1108.4   **Scientific Equipment**: Scientific equipment; Sharing (maintenance funding); Inventory (over $X)

S-1108.5   **Research Support Services**: Research support services; Site licenses; High performance computing; Memberships/subscriptions; NJEDge.Net, Internet2, etc.

The Process

The current charge was issued before the integration with UMDNJ was finalized, and therefore contains no information about the current state of the research infrastructure at that university. Nonetheless, the Committee is aware that leadership from Rutgers and UMDNJ are working together to address research support issues, and some of that work may overlap with the work of this Committee. Given this understanding, the Committee presents its recommendations as a checklist of issues that should be considered by the administrations both during and after the integration process.

For each of the subcharges, the Committee enlisted experts from the University's leadership to provide information and facilitate discussion in their respective areas. Testimonies were followed by Q&A, and in some cases, discussions and speaker follow-up between Senate meetings. The speakers were as follows:

S-1108.1   Grace Agnew, Associate University Librarian for Digital Library Systems; Charles Hedrick, University Director for Instructional and Research Technology and Chief Technology Officer; Peter Mattaliano, Director of iTV and Distance Learning - Center for Online & Hybrid Learning and Instructional Technologies; Silvia Muller, Instructor - Center for Online & Hybrid Learning and Instructional Technologies); Donald Smith, Vice President for Information Technology and Chief Information Officer

S-1108.2   Charles Hedrick; Tibor Purger, Director of Integrated Information Systems, Rutgers University Libraries; Donald Smith

S-1108.3   Frank Forte, Director, Telecommunications – Office of Information Technology; Charles Hedrick; Donald Smith

S-1108.4   Charles Hedrick; Tom Richardson, Associate Director - Office of Research Alliances; Donald Smith

S-1108.5   Charles Hedrick, Donald Smith

Introduction

Central to the University's research mission is accurate and secure data, in many formats, which can be efficiently and safely stored, organized, transported, preserved, and shared. Data must be managed so as to ensure security and compliance with government and funding agency regulations. Scholars need the right equipment and instrumentation, useful physical facilities, and access to archived information, as well as platforms and tools for collaboration. In the current underresourced environment, a high level of efficiency is required, as well as a well-informed community of scholars.

Furthermore, the advent of the Digital Humanities (DH) introduces a new and rapidly expanding field of information technology to higher education. Covering all of the contemporary humanities as well as classical studies and archeology, DH brings digital archives (written, spoken, graphic, digitized art images and musical) to the academy, and opens up new possibilities for integrating GIS with archived databases to inform humanistic investigations. Important questions arise related to security and access to these images.

Over the course of the Committee's discussions on the various services that comprise the University's research support infrastructure, it became clear that the Rutgers research community is often unaware of available capacity, services, and issues surrounding data storage, transport, and sharing. The Committee's recommendations derive from the need for increased coordination, education, communication, and compliance. By addressing these issues, the University can potentially realize significant cost savings and enhance opportunities for information, equipment, and instrumentation sharing.

For example, Rutgers research data is currently stored in scattered locations, including researchers' offices and homes, and departmental servers. This creates an environment where responsibilities for data storage, backup, migration, preservation, privacy protection, compliance, and security can be ambiguous or neglected. For the University's scientific equipment, there is no comprehensive inventory, adequate technical support, or mechanism to track depreciation or fund replacement. Similarly, content, in the form of databases, subscriptions, media, and the University's own scholarship, represents a major University investment, yet a lack of coordination in purchasing inhibits information sharing and increases costs through duplicate purchases. For site licenses, too, there is no mechanism to know what licenses are held and what is available to faculty across units and campuses. Finally, it is worth pointing out that the plethora of email systems across the University challenge the ability to comply with federal regulations related to privacy, record retention, and security breach notification. These are key examples of research support infrastructure issues at Rutgers, and all of them should be addressed. In fact, this fragmentation and redundancy may represent an opportunity to achieve significant cost savings. In any case, a program that is efficient, secure, and compliant is critical to the University's status as a major research university, and its ability to attract premier scholars and students. Addressing these issues should become a priority and ought to be integrated into the strategic planning process.

On the upside, Rutgers has made inroads in the areas of high performance computing and network technologies. "Big data," large-scale analytics, and computational modeling and simulations are playing an increasingly important role in industry. Businesses recognize the value of these activities and have made significant investments in both computational infrastructure and research and development activities. Rutgers has two high performance computing clusters, each of which seeks to expand the use of advanced computing while leveraging the economies of scale that come from centralizing networking, storage, power, cooling, and staffing. In addition, Rutgers was one of the early participants in the Internet2 consortium, alongside other public AAUs and Committee on Institutional Cooperation (CIC) schools. The primary goals of Internet2 are to create a leading edge network capability for the national research community; enable revolutionary Internet applications; and ensure the rapid transfer of new network services and applications to the broader Internet community. Through its participation in Internet2, Rutgers has discounted access to a number of important storage, collaborative, and videoconferencing services.

In the area of data sharing, the Rutgers University Libraries develop, host, and maintain the Rutgers institutional repository, RUcore, a widely available, centralized, searchable database of Rutgers' scholarship, research data, and digital archival materials. Original research products and papers of the faculty and administrators, as well as the unique resources of the Libraries, are deposited in the repository, where they are crawled by Google, easily retrieved, and permanently preserved. In addition to the repository itself, the Libraries offer a suite of tools and services to advance research and foster interdisciplinary collaboration. The Libraries have considerable expertise and are recognized leaders among our peers for data management and access strategies. The Libraries have a critical role to play in not only managing the data and scholarly literature produced by the research process but in supporting the research process at every stage. RUcore tools and services can increase research impact, improve communications of research results, and that can be readily extended to other departments, thus achieving economies of scale.

With the integration of UMDNJ, a new University president, a strategic planning process that is well underway, and entry into the Committee on Institutional Cooperation, the University is now at a crossroads with a tremendous opportunity to leverage these advantages, find solutions, and move Rutgers forward into a future of unparalleled success.

Recommendations

The University's research support infrastructure continues to reflect unwarranted fragmentation and a lack of security, both of which could potentially impact the institution's status as a research university and expose the organization to risk.

To address these issues, the University should:

- Educate scholars in available research support infrastructure capacities and services;

- Provide access to services and facilities for the storage, backup, and preservation of research data to allow researchers to meet their ethical and legal requirements;

- Provide, communicate, and enforce policies to ensure data security and compliance;

- Provide access to training and support in research data and records management;

- Explore ways to reduce fragmentation in the areas of 1) data storage and management; 2) purchasing and maintenance of equipment and instrumentation, site licenses, and content such as subscriptions and databases; and 3) video services.

The Committee believes that the University should establish a working group to look at existing services and researcher needs, and develop a plan for assessing what services should be provided and how to provide, support, and publicize them. This could be a coordinated effort between the Office of the Vice President for Research and Economic Development, the Office of Instructional and Research Technology, and Rutgers University Libraries.

The Committee also believes many of the issues stem from the dichotomy that exists between the administrative and academic sides of the house. Therefore, the Committee recommends that, where possible, the University strive to combine faculty and administrators on any committees formed to address these issues. Moreover, many of these issues span research and teaching missions and should be addressed in a holistic manner that takes both research and teaching into account.

Finally, the Committee makes the specific recommendations below; the rationale is discussed in the section that follows.

1. Expand the Libraries' role in research data organization, management, and innovation, and increase awareness of RUcore, the institutional repository, for storage, preservation, access, and management of Rutgers scholarship, research data, and conference proceedings [S-1108.1]

2. Perform a comprehensive analysis of services, needs, opportunities, and costs associated with video for research [S-1108.1]

3. Explore greater coordination of the acquisition and management of content, including media, databases, subscriptions, and the University's own scholarship, and determine appropriate means for funding them [S-1108.1]

4. Ensure that research data are stored on more centrally-administered computing systems that are managed using up-to-date protocols to ensure data security and

compliance with all relevant federal regulations, including those for disaster recovery and business continuity [S-1108.2]

5. Review, update, communicate and enforce policies for research data security to augment policies for general data security [S-1108.2]

6. Provide a required data security tutorial for researchers, and consider incorporating this information into the existing IRB (Institutional Review Board) Human Subjects Certification Program [S-1108.2]

7. Promote creation of effective data management plans for all research data [S-1108.2]

8. Establish a mechanism for coordinated long-term planning for network availability and use [S-1108.3]

9. Review, update, communicate and enforce policies for data transport as they apply to both wired and wireless networks [S-1108.3]

10. Ensure security plans are in place to address research data and data transport issues at the department and unit level [S-1108.3]

11. Provide a required data transport tutorial for researchers, and consider incorporating this information into the existing IRB (Institutional Review Board) Human Subjects Certification Program [S-1108.3]

12. Create, communicate and enforce a physical document transport policy for documents containing sensitive research data [S-1108.3]

13. Explore the possibility of a widely available, centralized, searchable database of specialized scientific equipment and instrumentation of significant value [S-1108.4]

14. Address funding issues for equipment maintenance, depreciation, replacement, and support [S-1108.4]

15. Explore the possibility of a widely available, centralized, searchable database of site licenses, and an appropriate means of funding them [S-1108.5]

One caveat to these recommendations: The Committee cautions the University that issues of responsiveness and governance should be considered when contemplating centralization of services and support, to ensure that researchers continue to have the tools necessary to pursue their scholarship.

S-1108.1 - Data and information sharing

1. **Expand the Libraries' role in research data organization, management, and innovation, and increase awareness of RUcore, the institutional repository, for storage, preservation, access, and management of Rutgers scholarship, research data, and conference proceedings**

2. **Perform a comprehensive analysis of services, needs, opportunities, and costs associated with video for research**

3. **Explore greater coordination of the acquisition and management of content, including media, databases, subscriptions, and the University's own scholarship, and determine appropriate means for funding them**

RUcore

RUcore, the University's institutional repository, with its suite of tools and services, can be extended to every department to meet their unique research creation and dissemination needs, much as the Libraries select resources and teach information literacy specific to each discipline.

Through RUcore, the Libraries can capture, describe, store, preserve and disseminate information in any discipline. They can store and manage, describe, and document the lifecycle of research data in any format, whether the data are raw, edited, or repurposed. They can link different versions of data, and link publications to their underlying data, whether held in RUcore or not, and embargo or restrict access to data as required by IRB or other needs. RUcore provides subject-specific portals where research can be gathered, and where scholars from around the world can coalesce and collaborate as communities of practice in a research area. In addition, the Libraries can work with faculty and departments to increase the impact of data, increase the innovation in terms of data management and access for grant proposals, and take responsibility for the ongoing management of data produced within a department. This is an area of excellence that Rutgers should leverage, as it does the many areas of research excellence at the University. Moreover, this capability needs to be more widely communicated to the Rutgers research community.

Media and databases

Rutgers University Libraries acquire many indexes, databases, electronic journals, electronic reserves, and other full-text resources through commercial licensing agreements that allow access to students, faculty, staff, onsite users, and authenticated offsite users. While the Libraries purchase many databases that are available to the entire Rutgers community, many others are purchased at the department or school level. These resources are available within the unit making the purchase, but there is no mechanism to make other units aware of the resource. This inhibits sharing of resources and may result in duplicate purchases. Moreover, funding is "catch as catch can" (for example through research funding) rather than strategic. Databases represent just one type of decentralized or fragmented resource acquisition; there are also others, including media resources.

Video and videoconferencing for research

Research applications of video are increasing at the University, as more and more researchers turn to video production and conferencing for research and collaboration with colleagues at other institutions. Some granting agencies are requiring production of video materials to provide access to research findings for non-scientists. Simulcasting and recording of conferences is becoming the norm, but a common understanding of copyright issues for recording, preserving, and disseminating video remains a challenge.

Video represents another area of fragmented and overlapping services, with numerous units involved in one or more aspects of video production, simulcasting, streaming, equipment provision,

training in video production applications, storage, management, dissemination, consultation, etc. To cite a few examples: The Office of Instructional and Research Technology (OIRT) provides video production for events, conferences, and overflow rooms; simulcasting and live streaming using desktop and room-sized videoconferencing technologies; access to the Rutgers YouTube and iTunesU channels and the State's NJVid streaming video server; and faculty and staff training in iMovie, Final Cut, Camtasia, and Windows Movie Maker, all of which are used to create research-based video materials. OIRT also produces the Faculty Research Spotlight and Undergraduate Research Spotlight, highlighting research conducted at the University.

The Division of Continuing Studies provides broadcast-quality recording of lectures, conferences, and special events. The unit produces documentaries; consultation on program and production planning on a range of multimedia projects; digital and analog satellite uplinks; fiber optic connectivity to global broadcast networks and television facilities; copyright guidance; and video streaming.

The Libraries develop, host, and manage the institutional repository, and thus provide a means to document, preserve, and make accessible video conference proceedings, the "new grey literature." The Libraries produce videorecordings of some conferences held in the Libraries, and advise Rutgers conference organizers on the necessary rights, permissions and recording standards, just as they consult on copyright and licensing issues in any scholarly publishing or associated projects. Videorecorded conference proceedings, as well as all research video, can be archived in RUcore, where they are crawled by Google, preserved over the long term, and managed for access and preservation through Libraries-supplied metadata. In addition, the Libraries provide reformatting and streaming services, as well as video editing and production equipment and training.

S-1108.2 - Secure Data Storage

4. **Ensure that research data are stored on more centrally-administered computing systems that are managed using up-to-date protocols to ensure data security and compliance with all relevant federal regulations, including those for disaster recovery and business continuity**

5. **Review, update, communicate and enforce policies for research data security to augment policies for general data security**

6. **Provide a required data security tutorial for researchers, and consider incorporating this information into the existing IRB (Institutional Review Board) Human Subjects Certification Program**

7. **Promote creation of effective data management plans for all research data**

Data storage and security

The ability to share data is fundamental for the operation of a research university. The need to store that data securely is the responsibility of everyone involved in research, including student, faculty, and staff researchers, and the university as a whole. The balance between sharing and limiting access to data is a delicate one, and an important consideration when creating university policies.

Currently, Rutgers research data are stored in many places, including researchers' offices and homes, on portable flash and hard drives, tablet computers, laptop computers, desktop computers, mobile devices, and departmental servers. There exist a myriad of ways in which these data can be compromised or lost. A laptop, tablet, or smartphone containing sensitive information may be stolen or misplaced; it can suffer physical damage, such as water damage; a locked file cabinet may be left open or opened by an unauthorized person; or sensitive information might be inadvertently posted on a web site without access restrictions. Any computer or server system compromise raises questions as to the continuing confidentiality of the data. Researchers are generally unaware of measures to prevent research data security breaches, and breaches are typically discovered after the fact. Moreover, researchers at times use cloud storage without fully understanding the data security implications of storing data in other countries.

This environment, wherein data may be stored abroad "in the cloud" or on servers purchased, housed, and maintained locally, and with insufficient accountability, is cause for concern. There are significant risks associated with this widespread practice, which results in dispersing responsibilities for migration, preservation, backup, privacy protection, and security. In addition, the costs of purchasing and maintaining servers in numerous locations (locations often not intended for this use) is significant. Further, many Rutgers researchers lack a full understanding of research data security issues. Therefore, to fully address data storage and security issues, the University must address both compliance and communication. The University needs to gain some control over cloud storage. A more centralized system of computing storage would help to ensure data security and federal compliance, although any increased centralization must address issues of governance and responsiveness. In addition, there must be a coordinated effort to clearly communicate the issues to researchers.

Data management plans

The National Science Foundation is now requiring that researchers create data management plans to ensure that data are usable, broadly available and sustained for long term access. For all researchers, a well-thought out approach to data management also saves time and frustration, maximizes the impact of the research, and is an important component of the responsible conduct of scholarship. A data management plan can help increase research efficiency, simplify the use and reuse of data, increase research visibility, meet funding agency requirements, and preserve data in the long term, thus allowing future scholars to build on Rutgers research.

RUresearch, a portal of RUcore, meets all the areas identified in the NSF guidelines for data management, including preservation, sustainability and metadata, not just for data sets but for accompanying research products. The Libraries' RUresearch Data Team provides consultation services on data management plans, archives data and products of Rutgers faculty research, partners with faculty on larger digital infrastructure projects and grants, and works on building the Libraries' capacity to archive and manage data. Nonetheless, this capacity is not widely known within the Rutgers research community. Researchers need a broad understanding of the tools available to them, and RUresearch services and capacity should be more widely promoted.

S-1108.3 - Data transport

8. **Establish a mechanism for coordinated long-term planning for network availability and use**

9. **Review, update, communicate and enforce policies for data transport as they apply to both wired and wireless networks**

10. **Ensure security plans are in place to address research data and data transport issues at the department and unit level**

11. **Provide a required data transport tutorial for researchers, and consider incorporating this information into the existing IRB (Institutional Review Board) Human Subjects Certification Program**

12. **Create, communicate and enforce a physical document transport policy for documents containing sensitive research data**

To support the research mission of Rutgers, the University must have a robust and reliable data, video, and voice network. The current network spans all three campuses and has connections to the Internet in Philadelphia and Newark, ensuring virtually uninterrupted Internet connections for university faculty, students, and staff. The university network is designed so that there are minimal interruptions to service and that if one part of the network fails, the remainder of the network will remain active. A mechanism for coordinated long-term planning for network availability and use will ensure the network remains a viable component of the university's infrastructure.

Information transported over networks must be considered to be at risk of being misdirected or monitored. Recently this risk has significantly increased because of the ever-increasing popularity of wireless networks, public Internet access services such as Internet cafés, and new Internet-based services such as cloud computing. Wireless networks are particularly risky since radio waves are not confined to secure areas. There is significant risk for monitoring even where wireless networks are not involved. The user could be accessing the Internet through an Internet café or hotel network. It is less likely that environments of this type will have professional network managers that would have the inclination and tools to check for illicit network monitoring devices on their network. In addition, other communication or collaboration solutions (SMS/text-messages, or public instant-messaging solutions like AIM, Yahoo messenger, Microsoft Messenger, etc.) can present an eavesdropping risk if the communication is not encrypted.

One of the areas of data security that often remains overlooked is data transfer. Although the network has mechanisms to deter security breaches, the methods by which researchers transfer data from home computers to work computers, from portable devices (like Android and Apple iOS tablets and smartphones), and from external hard drives and thumb drives are far less secure and much more likely to cause data integrity issues related to:

- Data transport within the Rutgers network
- Domestic data transport
- International data transport
- Non-electronic data transport

Data transport using the wired Rutgers network is generally secure. Using wireless networks, however, poses a number of risks. Anyone within a limited geographical range of an open, unencrypted wireless network can capture and record what is sent over the network and then use the information and resources in inappropriate ways. Departments, units, and individuals creating wireless networks must be made aware of what they need to do to maximize data security. Simply logging out of wireless connections and using complex passwords are not enough. The university's Office of Information Technology has a set of guidelines for creating and using wireless networks, including the use of firewalls and encryption of wireless routers.

Domestic data transport occurs daily between researchers' home computers and their office computers, between mobile devices and computers, and between laptop computers and desktop computers. Significant data security issues arise when individuals store research data on personally owned devices. Unless the device is connected to a Rutgers wired network, and access to the device is controlled, researchers are creating optimal conditions for data integrity breaches. Each of these transfers raises security risks, including, but not limited to, data theft and data corruption. In addition, many researchers analyze or collect data in wireless cafés or other places providing wireless services, further increasing risks to data integrity. One way to increase security when sending data between devices is to use a Virtual Private Network (VPN). A VPN uses encryption and other mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. IT staff in most departments can assist researchers in using VPNs for data transfer.

Crossing international boundaries creates even more opportunities for security breaches. Faculty and other researchers often travel without considering risks to their devices and to the confidentiality of the data that are on them. For example, hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched. All information that is sent electronically – by fax machine, computer, or telephone – can be intercepted and belongings are often searched multiple times when traveling. The likelihood of an electronic device being compromised is high (e.g., traveling to a country that is known to infect systems on their networks) and the impact of a confidential research data compromise could affect the university's opportunities to obtain research grants.

Standard data transport precautions include:

- Removing any data not needed while in another country to minimize the exposure should a laptop or mobile device be stolen, and if possible, carrying a "clean" laptop that does not contain confidential data;

- Using a Virtual Private Network (VPN) to connect to a Rutgers server to collect, store, and access the data;

- Not using portable equipment, such as flash drives, CDs, PDAs, phones, etc. to store or transport sensitive data;

- Creating strong passwords for cell/smartphones and never storing passwords on any device or in its case;

- Ensuring that all the information and software on a laptop can be safely and legally transported to another country since information, technology, software, and equipment may be subject to U.S. export control laws.

Finally, we oftentimes forget that not all data are electronic, and unfortunately, neither Rutgers nor any other universities have looked adequately into non-electronic data transport. Many researchers

use paper documents that might contain sensitive data from surveys, interviews, and research notes. While most researchers know how to secure the data for storage purposes (locked file cabinets in locked rooms), a smaller number think about how the data get from place to place. A policy and educational program might include issues such as document shredding, security issues surrounding fax machines and photocopiers, and the need to have sensitive data with the owner at all times (not locked in a car, for example).

S-1108.4 - Scientific Equipment

13. **Explore the possibility of a widely available, centralized, searchable database of specialized scientific equipment and instrumentation of significant value**

14. **Address funding issues for equipment maintenance, depreciation, replacement, and support**

In fiscal year 2010, more than $433.9 million of research at Rutgers was sponsored by the federal government, state government, corporations, and foundations, providing research experiences for undergraduates, supporting graduate assistants and postdoctoral researchers, and bringing state-of-the-art equipment and facilities to our campuses. Given this volume of research, it is surprising that the University maintains no comprehensive, centralized, and accessible equipment inventory. The Purchasing Department generally collects information about equipment purchases as items are received, in compliance with federal grant requirements, but unfortunately there are many exceptions, and no valuation is provided, particularly in terms of depreciation and planning for replacement. The Office of Research Alliances also maintains an inventory, but it is market-based, aimed at external clients, and built organically rather than strategically or comprehensively.

Researchers often do not know what equipment and instrumentation is available, even within their own units, and frequently there is no mechanism to upgrade equipment. A centralized equipment inventory could reduce siloing of equipment, minimize unnecessary purchases, and provide a systematic means to identify possible partnerships and share equipment. Ideally it would include contact person, price, access policies, rates, and mechanisms for sharing, etc., and encompass issues such as use tracking, compliance, accounting procedures, oversight, and management. Such an inventory could be a model for, or include, other inventories, such as for biological/scientific research materials.

The second scientific equipment issue pertains to funding for equipment depreciation, replacement, maintenance, and technical support. There is no mechanism to track depreciation in order to plan for and fund equipment replacement; those familiar with the equipment often lack the time to assist others in its use; and there are no mechanisms for departments to exchange funds when cross-departmental use of equipment does occur. Other universities institute user fees, but even where Rutgers has such fees, there is no enforcement. It is the Committee's understanding that the University prohibits use of user fees to fund replacement equipment, which would depreciation unaccounted for. We have also been advised that Rutgers is at the bottom of the scale in terms of technical support for scientific equipment, which has ramifications for safety. The lack of equipment maintenance and support can threaten Rutgers' standing as a premier research institution, and potentially could create significant liability issues for the University.

In the course of the Committee's work, a number of proposals were made in these areas, as follows. Many of these policies and procedures are already in place at universities such as Lehigh and Drexel.

- Establish a mechanism to track depreciation in order to plan for fund equipment replacement

- Develop benchmarks for adequate technical support for scientific equipment

- Allocate a percentage of the indirect monies from grants to support maintenance contracts

- Permit buyback of faculty time, as is standard at other research institutions

- Consider instituting and enforcing user fees for equipment

- Allow for technicians to be hired and funded by multiple departments

One final note: Although the topic of physical facilities was not included in the charge, the Committee feels strongly that if Rutgers is to maintain or increase its status as a major research university, it must become more attentive to its physical research facilities. In particular, University Facilities needs individuals possessing a body of expertise in laboratory design, and an understanding of design in the research laboratory context. This applies to both lab design and lab support services. This is another area where the University must build a bridge between its administrative and academic communities.

S-1108.5 - Research Support Services

15. Explore the possibility of a widely available, centralized, searchable database of site licenses, and an appropriate means of funding them

The acquisition of software licenses represent a tremendous amount of purchasing dollars, yet there is currently no effective way to assemble knowledge of what departments and individuals are purchasing and what is available to faculty. Funding for university-wide software site licenses is gathered on an ad hoc basis, often with a single staff member going to department chairs and deans "with a tin cup" to try to collect enough money to purchase licenses or arrange for bulk purchasing. This model is not sustainable and severely limits the university's potential for enhancing use of academic and research software.

Significant savings could be accrued through the process of university-wide software site licensing and bulk purchasing. A software collection development process, similar to the Libraries collection development process, in which information gathered from departmental faculty is used by Library faculty to develop discipline-specific collections, could be used at the University level to enhance academic and research software availability. As faculty identify software that they believe would have widespread use at Rutgers, the goal would be to match combined interests, potential needs, and purchasing power with vendor-specific educational pricing arrangements, to make more opportunities available to the Rutgers community.

Research, and Graduate and Professional Education Committee

Otto, Jane, Libraries (F), Co-chair
Stein, Gayle, NB Staff, Co-chair
Abu El-Haj, Thea, GSE (F)
Buchholtz, Ann, RBS:N/NB (F)
Cachel, Susan, SAS-NB (F)
Chant, Robert, GS-NB (F)
Clear, Todd, SCJ Dean (A)
Dantzler, Prentiss, GS-C (S)
DeLisi, Richard, Dean GSE (A)
Geerdts, Megan, GS-N (S)
Goodman, Robert, SEBS Dean (A) - *Administrative Liaison*
Greenhut, Victor, GS-NB (F)
Hackworth, Rhonda, MGSA (F)
Harris, Richard, FAS-C (F)
Holzemer, William, Nursing Dean (A)
Hudson, Judith, SAS-NB (F)
Jimenez, Leslie, SAS-NB (F)
Kukor, Jerome, GS-NB, Dean (A)
Lewis, Jan, Acting Dean, FAS-N (A)
Li, John, Engineering (F)
Maher, Ali, Other Units-NB (F)
Mao, Zhengyu, GS-N (F)
Moran, Kimberlee Sue, Camden Staff
Mullen, Jeffrey, Law-C (S)
Ottomanelli, John, Alumni Association
Pritchett, Wendell, Camden Chancellor (A)
Rodgers, Yana, GS-NB (F)
Schulman, Rebecca, GSAPP (S)
Sorensen, Lars, GSE (S)
Taghon, Gary, Other Units-NB (F)
Tancs, Linda, Alumni Association
Tsakalakos, Thomas, Engineering (F)
Weigert, Laura, GS-NB (F)
White, Carolyne, GS-N (F)
Zimmerman, Dean, SAS-NB (F)