Battening the Hatches

Report of the GMU Task Force on
Information Security and Privacy

March, 2000

EXECUTIVE SUMMARY

George Mason University has invested heavily in information technology to support its instruction and research. GMU's information infrastructure serves about 31,000 users on three campuses. GMU faculty and students are heavy users of instructional IT: 35% of courses use web pages to distribute course materials and resources, 85% use email, the Student Technical Assistance and Resource (STAR) center had 10,000 student visits in 1999, and the Instructional Resources Center is consulted by 60 faculty a month.

In the past several years numerous security incidents have affected GMU systems. Most incidents were limited in scope but expensive for a small group; a few affected many users. The number of these incidents has quadrupled in the past year. With our current state of readiness, a serious breach of our systems is possible and would be devastating to large numbers of students, faculty, and staff. Moreover, such a breach would seriously harm our public reputation as a leading university in the use of IT to support teaching and research. We can ill afford to sit back and take no action to reduce our vulnerability.

The task force identified sixteen major risks in four categories: identity, privacy and intellectual property, systems, and authentication. We concluded that GMU can achieve a substantial decrease in risk by adopting a coordinated set of measures in four areas: information policy, systems, people, and authentication. All recommendations can be implemented within nine months.

Our highest priority recommendation supports all four areas: That the VP of IT move rapidly to hire a senior professional as Chief Information Security Officer, who would head up a new Information Security Office within UCIS. The CISO would conduct a security risk assessment at least once annually, plan actions to address the risks, and coordinate all units to maintain a low-risk IT infrastructure. We further recommend that GMU acquire a state-of-the-art intrusion and vulnerability detection system to support the work of the ISO

(estimated at $125K for the first year and $20K for maintenance). These are the only recommendations requiring new resources.

All our other recommendations can be implemented from resources already allocated. We believe that the costs of implementing these measures are modest and are outweighed by the savings in reduced frequency and severity of incidents that will follow the implementation.

Our main recommendation regarding information policy is that GMU adopt an information policy. We have provided a draft.

Our main recommendations regarding systems are that GMU (1) adopt a set of management practices for certifying systems and system administrators, and for tracking systems and their IP addresses; (2) define minimum standards for every system connected to the GMU network and codify them in a computer security guide for users and system administrators; (3) make it a strict policy to keep all systems up to date with security patches that close known vulnerabilities; (4) institute practices of red teams, vulnerability scans, intrusion detection, and change management to deter attacks by locating vulnerabilities before hackers do; and (5) adopt the SANS Institute guidelines for incident handling.

Our main recommendations regarding people are that GMU (1) adopt the USENIX guidelines for the responsibilities of system administrators and definitions of their skill sets; (2) develop a program to certify system administrators; and (3) establish a set of user education programs to help users contribute to the maintenance of low-vulnerability systems.

Our main recommendation regarding authentication is that GMU set a goal to provide an authentication service and establish an engineering task force to evaluate alternatives and design the service.

Maintaining security should be a necessary cost of doing business. Given the growth of attacks on our abilities to do business, information system and network security is a cost that failure to pay can severely impair the business. This may be our last opportunity to secure our systems by fixing basic problems before we experience a really costly event.

Table of Contents

GMU Task Force on Information Security and Privacy

Membership

Peter J. Denning (chair), *CS*

Info Policy Subcommittee:
Anne Marchant (chair), *CS*
James Finkelstein, *TIPP*
Robert Hartman, Student, *SoM*

Systems Subcommittee:
John Hanks (chair), *UCIS*
Richard Jackson, *UCIS*
David Jensen, *UCIS*
George Sokol, *DoIIIT*

People Subcommittee:
Ron Secrest (chair), *UCIS*
Sandra Buckles, *IT&E*
Frank Blechman, *ICAR*

Authentication Subcommittee:
Wally Grotophorst (chair and liaison), *University Libraries*

Advisors:
Eric Sas, President, *GMU Student Government*
George Prokop, Corporate Systems Manager, *CFC*
Jeffrey H. Matsuura, Counsel, *Alliance Law Group*
Edward H. Bailey, III, Information Asset Security Officer, *Lockheed Martin*

Battening the Hatches

Report of the GMU Task Force on
Information Security and Privacy

March 2000

1 Introduction

1.1 GMU Environment

In 1991 George Mason University undertook to become a leader in the use of information technology and networking to support education and research. The Instructional Development Office was started in 1991 to locate and evaluate new technologies that might be useful in instruction and to assist faculty in learning to use these technologies. Every member of the GMU community -- faculty, staff, and students -- was given a permanent email address in 1994. The GMU network was upgraded to all-fiber optics in 1996. With all this connectivity, the demand for IDO's services grew so strong that in 1998 IDO and several related offices were merged into a single unit, the Department of Instruction Improvement and Instructional Technologies (DoIIIT). At the same time, all information technology units, including DoIIIT, were consolidated into the IT Department headed by the new Vice President for Information Technology.

At the beginning of 2000 there were about 31,000 user accounts on computers managed by UCIS:

22,900 students
2,300 student employees
765 full time faculty
4,300 other faculty and staff
1,200 guests

About 35% of the faculty maintained websites for distribution of class materials and resources and about 85% of the faculty used email communications in their courses. The Student Technology Assistance and Resource (STAR) center reported nearly 10,000 student visits in 1999, mostly to set up web pages for class assignments. The Instructional Resources Center (successor to IDO) averaged 60 faculty consultations a month. The usage of GMU IT resources is growing and will continue to grow as the new Technology Across the Curriculum initiative takes hold. About 30 professional system administrators and 60 part-time students support all this across the university.

To provide for the orderly and responsible use of this complex network, GMU established the Responsible Use of Computing (RUC) policy in 1994. This policy, developed through a campus-wide grass-roots process, was built on the principle that individual users are responsible for their own behavior in maintaining both

the security of the GMU network and the privacy of information in it. The policy adopted a "stopit" procedure to warn first-time offenders and give all users a standard means of reporting abuses. This policy has worked exceedingly well for a campus of this size. In 1997 about one complaint a week was submitted to stopit. By the beginning of 2000, the complaint rate had jumped significantly, to 20-30 complaints a week. About 85% of complaints are requests to stop spam, 5% requests to stop some form of harassment, and 10% reports on possible campus computer involvement in a criminal activity.

Stopit-reported incidents are, however, a small part of the overall picture. Many security incidents show up for users as interruptions or degradations of service -- for example, hijacked servers, viruses, blocked email, and denial-of-service -- and are reported to the Support Center rather than to stopit. Others are reported by users directly to their system administrators.

Many incidents have inherently high costs. For example, victims of harassment need coaching, counseling, and possibly police assistance. Considerable staff time is involved in each criminal investigation, whether staff are cooperating with the FBI on national investigations or with the campus police on local investigations. A growing number of campus computers are either hijacked to launch denial-of-service attacks, or are subjected to denial-of-service attacks themselves, especially when project and exam deadlines are imminent; dozens of staff hours are needed to reclaim each one of these servers. Computer viruses are a constant problem across the campus, regularly disabling computers and requiring expert help from UCIS staff to remove them. Even seemingly minor incidents can have major consequences, especially if left unattended. For example, failure to block spam relays within a few hours after they are reported is likely to lead to outside spam-monitoring organizations to "blacklist" GMU, effectively cutting off email service to the large number of organizations that honor the blacklist. In all, the cost of processing incidents is high and growing.

Here are examples of security incidents at GMU in the past few years; see also Appendix 5. In 1996 several system administrators were involved with the investigation of 12 incidents involving a student hacking ring in the IT&E school; this eventually led to court hearings and a dismissal of the case because the evidence (email logs) was not sufficiently tamper-proof to satisfy the court. In 1997 someone (possibly from the same ring) broke into the main engineering computers and deleted a large number of files and accounts during summer school, causing hundreds of students and faculty to lose up to half their work in summer school. In 1998 several UCIS staff were involved for several months for a substantial portion of their time in assisting law enforcement investigators with a student term paper and credit card fraud ring. In 1999 TIPP reported an incident in which hackers hijacked a server; it took them over a month and $10,000 consulting fees to reclaim it. In the same year, TIPP was also the victim of a password sniffer attack. In 1999 a Windows NT server in the Registrar's Office was hacked: many administrative and user accounts were compromised and a denial-of-service attack was launched against non-GMU sites; 15 people were involved in the investigation, which took about 80 hours total time to resolve.

GMU is not alone in experiencing rapidly escalating and expensive security incidents. The national CERT Coordination Center (cert.org) reports these national statistics for 1999:

- 33,000 email messages
- 2,100 hotline phone calls hotline
- 8,200 incidents (up from 3,700 in 1998 and 2,100 in 1997)
- 6,000 web hacking (defacing) incidents since August 1999
- 419 distinct vulnerabilities reported (up from 262 in 1998)

GMU's intrusion incidents mirror national profiles reported by the CERT Coordination Center. These include password sniffing, website hacking (including breakins via Common Gateway Interface and defacing of web pages), and distributed denial-of-service attacks. Hacker websites offer complete "burglar toolkits" that enable rank amateurs to mount sophisticated attacks. Our UCIS system engineers estimate that a substantial number of attacks would be eliminated completely if traffic on the GMU networks were encrypted, putting it beyond the reach of sniffers. They also estimate that website breakins can be significantly reduced by maintaining all websites with up-to-date security patches. Our ability to secure against these threats has been limited by the lack of a campus security plan and an Information Security Office to coordinate units and manage the plan.

In addition to concerns about attacks, there are widespread concerns about the privacy of information stored in GMU computer systems and transmitted on GMU networks. Sniffing technology can be used to read private documents in transit on the network. Inadequately managed computers become ports of entry for hackers. State mandates for providing information and forms on websites (see Appendix 2) create new ways for official information to be defaced and confidential information input via a website to be stolen. Many units are not aware of their responsibilities in the protection of information in their computers, and the campus provides no means of helping them validate that their computers meet all campus policy requirements for protection of information privacy.

1.2 Areas of Concern

On reviewing this situation, Joy Hughes, GMU's Vice President for Information Technology, concluded that GMU's vulnerability to attack and compromise was unacceptably high. She asked the Security Review Panel, which oversees the RUC policy and its implementation, to comprehensively review the security and privacy practices of the university and to recommend improvements and changes. The detailed charge to the task force is included as Appendix 1. The task force grouped the concerns behind the list of thirteen items in the charge into four categories:

Information policy

Concerns the kinds of information in our systems (e.g., confidential, public, personal, and other), standards for protecting each type of

information, and rights of access to each type of information. (It should be noted that although the university protects information and respects its privacy, it is obligated to release information when required by state or federal law. See Appendix 3.)

Systems

Concerns the computers and networks that store, transmit, and process information. Includes networking infrastructure, protections against common attacks, security standards to be met by campus systems, tracking which systems meet standards, enforcing standards, and alternative means to connect systems not meeting standards.

People

Concerns the qualifications of professional staff and student technicians who administer computers, and also the level of user awareness of their part in a secure campus. What does it mean to be a qualified system administrator? What process(es) should be used to qualify people for system administrator jobs? How should the user community be educated about their responsibilities and the consequences of irresponsibility? How do we investigate complaints and respond to law enforcement requests for help gathering evidence?

Authentication

Concerns the level of trust we can place in parties interacting with us. How do we know that someone is who he/she claims to be? How do we know that documents are authentic? How do we control access so that only authorized persons can sign electronic forms?

The task force organized itself into four subcommittees to address each of these areas. In addition, with the help of the Century Club, the task force recruited three security and privacy experts from regional businesses to advise the committee.

1.3 Findings and Recommendations

The findings and recommendations of the subcommittees follow in the sections below. Our recommendations emphasize principles rather than operational details. All them can be implemented in the next six months. All but two -- hire a Chief Information Security Officer and acquire intrusion vulnerability detection systems -- can be implemented within current resources.

The most important finding of the task force is that our vulnerability to attack and compromise is high and that our good fortune in avoiding serious problems is not likely to last much longer.

Because of the complexity of GMU systems and operating rules, and because improved security practices will require substantial work and coordination to implement, our first recommendation is that GMU move quickly to hire a Chief Information Security Officer and direct UCIS to establish an Information Security

Office. The CISO would be a senior person experienced in security and privacy, sensitive to the essentially open nature of a university campus, and capable of orchestrating all the components needed to implement information security and privacy policies across the university. We expect that the CISO would provide detailed operational plans for the principles set forth in our recommendations.

GMU's vulnerabilities can be significantly reduced through the measures recommended here. Fewer vulnerabilities will mean much lower risk of criminal activity, less inappropriate use of GMU information, and a much more reliable information infrastructure. The costs of maintaining our environment at its current level of readiness have been high and are escalating. The probable costs of future incidents will exceed the costs of implementing the recommendations herein.

2. Chief Information Security Officer

Because of the complexity of the campus network, the highly technical nature of computer security, and the need for coordination among all campus units, the task force recommends that GMU hire a Chief Information Security Officer and establish an Information Security Office (ISO) within UCIS. The CISO would be a senior person experienced in security and privacy, sensitive to the essentially open nature of a university campus, and capable of orchestrating all the components needed to implement information security and privacy policies across the university. The responsibilities would include:

- Annual risk assessment leading to an "information health plan" that addresses threats identified. The Security Review Panel (SRP) can conduct the assessment for the CISO.
- Periodic audit of computer networks and operating systems to uncover potential weaknesses from both insider and external attacks; defining and reviewing criteria for removing deficient systems from the network.
- Establishment of recommended backup and recovery procedures in the event of both large-scale and small-scale failures of critical systems.
- Periodic audit of the types of information managed by each units, their security and integrity procedures, and backup procedures.
- Oversight of information privacy policy and periodic audit of privacy related procedures.
- Continuing education of the university community in computer security and privacy issues in coordination with existing educational training resources.
- Management of an incident investigation and reporting process.

2.1 Recommendation

2.1.1 Hire a Chief Information Security Officer (CISO) and establish an Information Security Office (ISO) as soon as possible.

3. Risk Assessment

The task force compiled a list of the major risks that need to be addressed by our security planning and our security practice. Because we are an open environment with state-owned public computing resources, we have risks that do not normally appear in a corporate environment. The risks that dominate the concerns on this campus are in four groups:

Identity

- A significant, well publicized security event could damage GMU's reputation as a leader in the use of information technology.
- Legal suits may result from the lack of a clear information policy.

Privacy and Intellectual Property

- Sensitive information may be stolen, compromised, or damaged by intruders in computers connected to the campus network.
- The Commonwealth of Virginia has mandated that all forms used by our customers be on-line. Therefore, interactive web forms need to be on secure sites. Many forms are very sensitive and some, such as student evaluations of faculty, are not covered by privacy policies.
- Many users and campus offices are not sensitive to the possibility that confidential information displayed on improperly positioned computer displays might be observed by unauthorized persons.
- Some users download and store copyrighted materials (e.g., music and video) without licenses.

Systems

- All systems are subject to intrusions by outsiders; a compromised system is an easy port of entry to the rest of the campus network.
- Password sniffing and cracking are common attacks against campus computers.
- Viruses and Trojan horses are a constant threat to all computers.
- Denial of service attacks are increasing common; some are launched from hijacked campus servers and some are launched against campus servers.
- Significant degradation of campus network performance or system storage space can occur when users engage in disallowed but tempting activities such as being paid for watching ads on their browsers, setting up continuous news feeds, and downloading large music and video files.

Authenticity

- Access to databases must be limited to persons whose job responsibilities grant them a need to know.
- Senders of email and official documents can easily be impersonated.
- Signatures on electronic forms can be forged.
- Documents can be forged.
- Official web pages can be defaced or altered by unauthorized outsiders.

3.1 Recommendation

3.1.1 Establish a practice of conducting a campus risk and vulnerability assessment at least once a year. The assessment can be conducted by the Security Review Panel (SRP), which will advise the Chief Information Security Officer.

4. On-Line Electronic Services and Executive Order 51

In mid 1999, the Governor of the Commonwealth of Virginia issued Executive Order 51, which mandates that all state agencies make their current and expanded services available to their customers via the Internet. (Appendix 2.) Each agency must provide the Department of Information Technology (DIT) with an implementation plan by June 1, 2000.

Implementation of this order on campus will impact security and privacy. Most offices and departments will, if they have not done so already, have to provide copies of their forms via Web pages to students. Many will turn to interactive Web pages that permit students to enter data on-line. Web servers will need to be configured properly so that the information entered is immediately moved to a secure partition or database; the subdirectories of the web server are vulnerable to intrusion attacks against the web server. Web servers may need "watermark" or other signature capability to protect against intruders changing official forms or information.

Each unit offering on-line services will need to post, or link to, a privacy policy for information collected from its clients.

A major process affected by this order is the student evaluation of instruction. At present, student evaluations are collected on paper forms and the results are published on a GMU website accessible within the gmu.edu domain (ratings.gmu.edu). In courses where a substantial part of the business is conducted on-line, instructors may want to use interactive Web forms to gather the data. GMU has no policy that covers this process.

Because so many units are, or soon will be, storing sensitive records in on-line databases, GMU needs a records-management policy to define the responsibilities of the administrators of each of these systems. The policy needs to define formal "custodians" of electronic records. This is necessary to be able to establish a "chain of custody" and other elements of evidence integrity in case

of legal action. The policy needs to define acceptable principles and practices for data collection, retention, distribution, protection, and ultimate destruction of electronic records.

4.1 Recommendations

4.1.1 The VP of IT should issue guidelines for configuring web servers that dispense services and forms for protection and security of data stored there. These guidelines should address

- Configuring interactive web servers for security
- Watermarking pages and forms
- Disclosing privacy policy applicable to each site
- Responsibilities for "record custodians" of each database
- Data gathering, retention, distribution, protection, and ultimate destruction.
- Process for handling objections or grievances regarding the management of private information.

4.1.2 The VP of IT should work with the Provost and Faculty Senate to develop a policy for the process of student evaluation of instruction, given that reports are distributed on-line and data may be gathered on-line.

5. Information Policy Recommendations

This section is a draft of an information policy for GMU.

5.1 Statement of Purpose

This policy rests on three main guiding principles:

- Information is one of the University's vital resources. With the increased dependence upon computer systems and the expansion of computer networks for the management and dissemination of information, it is essential that University information systems and networks are protected and secure.
- The University has both a legal and moral responsibility to protect the integrity and confidentiality of certain kinds of records, including, but not limited to, student academic and health records, employee benefits and health records, confidential information in personnel files, and certain research activities.
- Procedures must be written and implemented to balance the need to protect privacy and intellectual property rights with the need for the open exchange of ideas that is the hallmark of the University environment.

The goal is that members of the University community will be able to exercise their discretion and best judgment when determining what and how to protect information for which they have responsibilities, within the legal constraints and other obligations of the University. Where procedures and practices are required, they are meant to be flexible enough to change as circumstances change.

5.2 Information Resources

The University gathers and maintains information for many purposes, ranging from student records to research data. Anyone who creates and maintains an information resource should develop a clear statement of the purpose for doing so, level of sensitivity, intended use, security and integrity plan, and plan for safe disposal when the information becomes obsolete. Various state and federal laws control the collection and use of certain types of data and the University is responsible for upholding these laws.

Information will be categorized as follows. The examples are not intended to be an exhaustive list.

Confidential

This category includes information to which access is restricted, usually on a need-to-know basis by job function with GMU. This includes student records and applications, course rosters, employee records (although dates of employment and salary are public records), security information (including passwords and authentication keys), research (until it is made public), and other information (such as draft manuscripts, student petitions and forms, internal memos, budgets, letters of recommendation, and correspondence) that is restricted to limited distributions within the university community.

Public

This category includes schedules, catalogs, inventories, statistics, University approved web pages (including course web pages), wages, and any other information intended for the general public.

Other

This category includes information that is not otherwise categorized, including personal files, memos, and email files.

While all information should be protected against loss by appropriate backup and recovery procedures, special safeguards must be in place to protect information deemed critical to the mission of the University.

In compliance with the Governor's Executive Order #51, units will make every effort to make routine forms and applications available over the Internet, including versions of forms accessible to the visually handicapped. Every effort will be taken to protect information entered into electronic forms. All new

information systems will be implemented in such a way as to be compatible with other University and state-wide systems as appropriate.

5.3 Responsibilities of the Information Security Office

The ISO should maintain and distribute guidelines for servers that dispense information services and forms for protection and security of data stored there. These guidelines should address

- Configuring interactive web servers for security
- Watermarking pages and forms
- Providing a privacy policy notice applicable to each site and database
- Defining responsibilities for "record custodians" of each database
- Data gathering, retention, distribution, protection, and ultimate destruction.
- Providing a process for handling objections or grievances regarding the management of private information.

The ISO should conduct periodic audits of the privacy policies and practices of on-line information services.

5.4 Responsibilities of University Community Members

All members of the university community are responsible for upholding the Responsible Use of Computing (RUC) policy and related policies in accordance with relevant state and federal laws. Any suspected compromise of University systems should be reported to the Unit Manager, Information Security Office, Security Review Panel (SRP) or GMU Police Department as appropriate.

Each unit is responsible for establishing internal procedures for maintaining its information, network, and computer system security. These procedures should satisfy university guidelines (maintained by the Information Security Office) with variations and additions as required for the unit's mission. Units are expressly charged with clearly identifying confidential or sensitive information within their unit and ensuring that employees understand the procedures needed to safeguard such information.

Faculty, staff and student employees are responsible for the information they create and maintain within the scope of their jobs. While it is recognized that mistakes can and will occur, every step should be taken to ensure data integrity and security.

5.5 Privacy Policy

- University web pages that gather information shall state or link to a privacy policy.

- The University will release confidential, private, or personal information only when compelled to do so by a valid legal order (for example, court order, subpoena, administrative law order, valid FOIA request).
- The University will not sell confidential or personal information. The University reserves the right to distribute and possibly sell aggregate information.
- The University will bear no responsibility for material unrelated to the University's mission added to a University system.

Anyone who requests users to provide personal information for a database must state clearly the purpose of the database and allow the person providing the information an opportunity to opt out of any external distributions of the information. Personal information in the database will not be released outside the University without informing the individual and giving the individual an opportunity to verify the accuracy of the information. If the database manager changes the distribution policy, all persons in the database will be given the opportunity to opt out or to withdraw from the database.

Searching one or more databases to link records and build profiles of individuals will be done only when there is a compelling need. In each case, privacy implications must be evaluated prior to implementation.

While the University respects privacy and confidentiality, and takes many steps to protect it, members of the campus community should understand that records may have to be released in compliance with valid legal orders such as a FOIA request or a subpoena.

The University is not responsible for private or personal information not related to the mission of the University. Persons who store such information or transmit it in campus networks do so at their own risk.

5.6 Reassessment and Revision

This policy should be reassessed annually by the Vice President for Information Technology periodically for effectiveness, cost, and flexibility. It should comply with State and Federal Law and with applicable campus policies. The review should include a comparison with the "best practices" other institutions of higher learning.

6. System Recommendations

The systems group concentrated on the vulnerabilities of GMU computer systems and networks. They identified three major security issues:

- Securing the Systems: Making systems as secure as possible, to thwart attempts to break into or compromise the system;

- Identifying the System Administrators: Identifying the person responsible for each system, including secondary contacts, to aid in dealing with systems that have been compromised; and
- Enforcement of Security Procedures: Proactive and Re-active procedures for dealing with the security of systems.

Taken together, the measures recommended below in these three areas would significantly reduce the exposure to attack and the costs of recovery.

6.1 Securing Systems

Five sets of concerns need to be addressed.

- Configuration. The initial "Out Of Box" configuration of a system needs to be brought up to GMU's minimum standards for connecting systems to the network. Configurations need to be maintained through maintenance, installing all required patches, removing services not required, and installing third party tools to detect and prevent compromises.
- Account administration. This includes everything from the use of good passwords to the proper permissions on files.
- Applications Security. This is making sure that the applications that are running are configured to provide the best security possible. TCP wrappers to restrict access to applications are a common example.
- Physical Security. This would be a guideline on how to protect systems from compromises that can be easily attempted by anyone with physical access to the system.
- Transmission of Sensitive Data. This includes the use of products like Kerberos for password authentication, secure shell (ssh) for remote login, and secure file transfer protocol (sftp). The word "sensitive" refers either to confidential or restricted data or to passwords and public keys.

Our recommendations:

6.1.1 Almost all the issues listed above could be easily resolved by specifying baseline standards and procedures in a *George Mason University Users Computing Security Guide.* Examples of baseline standards are:

- Rules for safe password selection, frequency of change
- Backup and recovery requirements
- Anti-virus requirements
- Security audit of new installations before attaching to the network
- No shared accounts
- Dormant accounts deactivated after 60 days

We recommend that UCIS create and maintain the *Guide* and that all GMU system administrators be required to use it. Most of the information in the guide would apply to every one of the 16+ operating systems on

University computing platforms with some sections customized for different platforms. A basic outline for the Guide is in Appendix 4.

6.1.2 We recommend that a system certification process be developed. The system certification process would be used to verify the security of a system prior to network connectivity being granted. It would be based on a security checklist. The process must define which systems ought to be certified (e.g., personal machines including dialup, laptops, and dorms as well as University equipment). The process must also define what measures, such as disconnection, would apply if a system is compromised.

6.1.3 We recommend that the most sensitive computer systems and databases (e.g., the Student Information System and the Human Resources System) be isolated from the main campus network by firewalls that restrict access and use strong authentication before granting access. UCIS should provide a means by which sensitive databases maintained by any organizational unit can be similarly protected.

6.2 System Administrators

Once a system has been identified as "secure", we need to know who will maintain it that way. We need to create a comprehensive system to tell who is responsible for each campus system, how to contact them, and who is the backup in case the primary contact is unavailable.

Our recommendations:

6.2.1 We recommend that a new structure for coordinating system administrators be instituted. The new system should include an intermediate level "area coordinators" who know how to contact restrict groups of system "owners". This might be accomplished by adding "Building Coordinators" to the existing 'Telecommunications Coordinators" and developing a hierarchy of support for locating and fixing problem systems.

6.2.2 We recommend the creation of a new database for identifying the assignment of IP addresses. Each record in this database would include:

> Permanent IP address, Hardware address, Type of machine, OS loaded, Location of machine, Owner of machine, System Administration, Department Coordinator, Building Coordinator, Serial # / Property #, a description of what the machine is used for, and system status.

This new system would be linked with the HRS system to update the user information when staff leaves. The system should also include an automatic yearly "renewal" of the IP address allocations to make sure that allocated addresses are still in use.

This same system could / should also be used to fill the existing need for both inventory and seat management that is required by UCIS. At a

minimum, there should only be one database that the others can be extracted from.

6.3 Enforcement

Once we have secure systems and trusted administrators, we need clear procedures for dealing with systems that do not meet our standards. We distinguish two categories of enforcement:

- Proactive enforcement: Identifying vulnerable systems before incidents occur or after they occur but before serious damage is done; and fixing those vulnerabilities before they are exploited.
- Reactive enforcement: Following standard, documented procedures for removing systems that have been compromised; and re-attaching those systems to the network after they are repaired and re-certified.

Our recommendations for proactive enforcement:

6.3.1 Aquire a system (hardware and software) to proactively "scan" all devices on the network to locate and identify known security holes. This will NOT be a replacement for proper System Administration. It is intended as an early-warning system for system administrators to help them confirm that their systems are properly administered and to locate systems requiring immediate attention.

6.3.2 Acquire an intrusion detection system. This type of monitor is most likely to be useful if deployed at the Internet gateway, between campus routers and on selected networks (such as dorms, dialup, or Thompson Computer room). (We estimate that the initial cost of a combined intrusion and vulnerability detection system is $125,000 and the annual maintenance cost is $20,000.)

6.3.3 Establish a "red team" reporting directly to the CISO; their job is to probe systems for vulnerabilities and report them with recommendations on how to eliminate them to system administrators.

6.3.4 For each of the measures recommended above -- scanning probes, intrusion detection, and red teams, develop guidelines for the use of the tools, reporting of results, notifying system administrators, and the personal ethical conduct of people who operate the tools or serve on red teams. Define levels of severity of vulnerabilities (minor, severe, critical) and grace periods for correcting them before a vulnerable system will be disconnected from the network.

6.3.5 Establish a process of change management: document deficiencies, risks, and solutions in a database shared by all system administrators. This system can detect if reconfigurations or installations have changed base settings and have created unacceptable vulnerabilities.

6.3.6 Develop a student group who implement, evaluate, and improve on custom tools for monitoring compliance with security standards. This would be a good way to involve aspiring system administrators in the

protection of our systems and to train them in the professional and ethical standards of system administration.

Our recommendation for reactive enforcement:

6.3.7 Create formal guidelines for GMU administrators on handling security violations. As part of this, adopt the forms and procedures listed in the SANS Step by Step guide for incident handling. This administrator's guide will advise on how to assess whether a compromise has occurred, how to identify the source, how to disable the system with the problem , and how and when to reestablish service, and how to respond if criminal activity is suspected. This guide is not the same as the sections of the User's Guide (Appendix 4) on incident handling.

7. People Recommendations

7.1 Assumptions

The subcommittee worked with this problem statement:

- The campus houses a large number of networked systems and servers. Some of them are not professionally or competently managed, potentially allowing intrusion into the GMU network and its associated systems. Resulting attacks may impede, impair, or deny service.
- GMU runs its systems with the help of about 30 professional system administrators and 60 student system administrators. The student administrators are not as experienced or mature as the seasoned professionals.
- Users may not understand security issues and inadvertently create security vulnerabilities. Also, many users have unrealistic privacy expectations.

Based on the charge of the subcommittee and the problem statement, the subcommittee investigated these issues:

- Duties and responsibilities of a GMU systems administrator (SA).
- Criteria for being a qualified SA at GMU.
- Process for evaluating and certifying systems administrators for different levels of authority.
- Procedure for investigating security related complaints and gathering evidence.
- Educating users concerning their responsibilities and the consequences of their irresponsibility.

Each of the areas of inquiry is defined in the following paragraphs.

Systems Administrator (SA) Duties and Responsibilities**.** The generic duties of an SA include: operating systems and software maintenance; accounts management; security management (maintaining system integrity and function);

data integrity (file backups and restores); and user education. The security management function includes monitoring the systems for abuse, installing security patches immediately on release, and investigating security complaints.

Criteria for Qualified Systems Administrators**.** Clear standards for competence are needed for system administrators, both for professional and student system administrators. (The university makes use of student assistants in many functions, including system administration.) Many departmental systems throughout the university are not properly managed and therefore pose a security threat to the department and to the university.

The standards need to address three areas of skills: vendor interface, user interface, and system interface. They need to set minimum requirements on continuing education and on-the-job experience. They need to specify a minimum amount of time per week that a system administrator is available to maintain and monitor a system.

System Administrator Certification and Evaluation**.** We need a process for certifying system administrators at different levels of skill and authority. We also need a process for the training and ongoing professional development of system administrators.

Security Investigations**.** Proper handling of investigations is needed to enable prosecution of criminals and safeguard evidence. Security incidents involving the engineering servers (hacking accounts), the Registrar's office (Denial of Service) and the Financial Aid Office (Web page defacing) led UCIS staff to conclude that standard university-wide investigation procedures are needed in order to adequately respond to security threats. These procedures need to address complaint investigation for major and minor infractions, gathering and protection of evidence, and interacting with law enforcement agents.

User Education**.** It is essential to educate the user community about their responsibilities and inform them of the consequences should they be irresponsible.

7.2 External Sources

To draw on the experience of security experts and professionals from academia, government, and private industry, we used three outside sources:

- "Incident Cost Analysis and Modeling Project" - A report from the CIC Security Working Group to the CIC Chief Information Officers. The project director was Dr Virginia Rezmierski of the University of Michigan.
- "Computer Security Incident Handling Step By Step: A Survival Guide for Computer Security Incident Handling" published by The SANS Institute.
- Publications on Systems Administration published by the USENIX Association for SAGE, the System Administrators Guild.

7.3 Security Incident Costs

Computer security incidents are usually costly. The Incident Cost Analysis and Modeling Project studied 30 IT-related incidents (source #1 above) resulted in calculated costs totaling $1,015,810. Cost variables in the model included dollars, employee time, number of affected users, and a few unquantifiable costs. Employee time is an opportunity cost representing lost productivity.

Currently, UCIS does not track costs related to security incidents.

Appendix 5 is a compendium of security incidents, each requiring significant effort to resolve, and many involving serious inconvenience or loss of work for many users of the affected machines.

7.3 Recommendations

7.3.1. Adopt as a guideline the "Computer Security Incident Handling Step By Step" published by The SANS Institute. A corporate license is available for $1,800 allowing the posting of the document in PDF format on a GMU internal website. These procedures should be augmented to conform to Commonwealth incident reporting requirements.

7.3.2. Adopt as a guideline three Systems Administrator publications from the USENIX Association. The publications are entitled: "Job Descriptions for Systems Administrators, 2nd ed.", "Hiring System Administrators", and "Educating and Training System Administrators: A Survey." These publications are available the USENIX Association for $7.50 each plus postage.

7.3.3. Develop and institute a university wide program to evaluate and certify systems administrators for different levels of authority. Such a program would be directed by the CISO.

7.3.4 Require an annual signed security agreement as a condition for use of GMU systems for the ensuing year.

7.3.5. Engage with the following methods for increasing user awareness of security issues, policies, procedures, their responsibilities, and the consequences of irresponsibility.

A. Conduct information security presentations at new employee orientation in Human Resources.

B. Conduct information security presentations at student orientation sessions and for Resident Assistants (RA).

C. Sponsor System Administration outreach programs.

D. Develop and distribute information security brochures:

- Paper brochures
- On-line security web page
- Posters in student labs

- Articles in the *Broadside* and *Gazette*: rules and regulations; incidents and consequences.
- *Broadside* interviews with GMU security experts on GMU security issues and implications.

8. Authentication Recommendations

The operation and academic mission of George Mason University requires ready access to a complex assortment of electronic information resources. These include:

- web pages (many official, e.g., class web pages, admissions, financial aid, policy statements)
- official documents and databases
- official communications
- records
- reports
- workflow
- interactive forms (e.g., web-based input)

These resources are numerous and extensive, distributed across three campus locations, and accessible to a very large community of users. The ability of the GMU community to carry out its missions depends on the accessibility, availability, authenticity, accuracy, and integrity of these information resources. Our users want such assurances.

At present it is impossible to give such assurances. Much of the information (especially the web pages) is stored on servers that do not have all current security patches applied; a determined attacker can break in to any of these sites and steal or tamper with the information they contain. It is quite simple for anyone to send email with a return address apparently from anyone else; it is increasingly difficult for users to determine whether an email message actually comes from the person named as the sender.

A growing number of units are turning to workflow systems to automate routine administrative processes such as signing and routing forms; we have no authentication system that guarantees that only authorized people can affix digital signatures to any of these documents. It will be impossible to scale current workflow applications up to the full campus without such a system. By the time the Oracle database systems are installed, a solution to this problem will be absolutely essential.

The Library's recent experience illustrates the problems in authentication, confidentiality, and integrity that arise in a large distributed information system:

> The library subscribes to several external database services. The license agreements with these suppliers restrict access to the university community. Non-GMU people, who have access to most of GMU's web pages, are not allowed access to these library

services. The library's first-generation solution to this problem was to place a monthly extract from the Registrar and a faculty-staff list on a validation server, which could then block access to outsiders. Within a year, the library had to use weekly extracts from the Registrar to cope with numerous changes in people's status. Installation and maintenance of the validation database has become very expensive. The library will soon confront a new requirement that will be even more labor intensive: regulating access to documents by course -- so that online course readings will be available only to students enrolled in a particular course. The library does not want to develop its own validation system, only to find it is incompatible with validation systems developed in other units. Instead, the library would like to have access to a university-provided, shared, real-time validation service.

Although much has been written in the press about the wonders of encryption technology, many critical aspects of this technology have yet to be reduced to reliable, cost effective practice. It would be wonderful if routine student forms could be digitally signed and routed via email, if digital Watermarks could be used to protect course materials posted to the Internet, if encryption could be used to prevent passwords from being transmitted in the clear over campus networks, or if smart cards and biometrics could be used for user identification. There are many practical problems involved with installation and configuration of appropriate card readers and encryption clients, protection and distribution of public keys, and management and distribution of smart cards. For these reasons we recommend that an engineering task force be chartered to properly evaluate authentication technologies and recommend those that will genuinely benefit the campus.

8.1.1 We recommend that the VP IT appoint an engineering group to design and develop an enterprise-wide authentication system. The charter for this group should include:

- Survey the current need for authentication, confidentiality and integrity across all users of the Mason network. Develop a matrix that shows the requirements for all major systems on our campuses. Pay particular attention to interoperability of systems when charting requirements.
- Evaluate competing technologies.
- Determine the implementation issues of each potential solution.
- Recommend a solution that addresses our needs and provides benefits to GMU users.

APPENDIX 1. Information Security and Privacy Task Force Charge

(By Joy Hughes)

Charge: To deliver, by 3/1/2000, a plan to improve the security of university computing systems and protect the privacy of data stored therein. The plan should address the following security issues plus others the Task Force deems essential to a secure computing environment:

1. Categories of data that the university manages in its computer and data systems, the standards of confidentiality and privacy accorded to each, and the units responsible.
2. Categories of trust accorded to servers attached to the campus network, standards for achieving trust categories, and standards for connecting servers to GMU networks according to their category of trust.
3. Access rights including prioritization of systems for public access, technical solutions to allowing open access to on-line forms without compromising security, etc.
4. User authentication and account management.
5. Authenticity of official communications, including ensuring solutions are congruent with the Commonwealth's standards and policies on digital signatures.
6. E-commerce: security and privacy of transactions between GMU and its customers especially its students.
7. Improving the management of change that affects system security including defining methods of coordinating configurations among central and distributed systems.
8. Academic Unit responsibilities including the selection, hiring, and assessment of system administrators and maintenance of servers at university standard security levels.
9. System administrator roles and responsibilities.
10. UCIS roles and responsibilities, including the possible establishment of a Chief Information Security Officer position and supporting staff.
11. Systems and procedures to respond to security intrusions, breakdown, and violations.
12. An ongoing community education plan.
13. Recommendation changes, if any needed, in the Responsible Use of Computing policy.

APPENDIX 2. Commonwealth of Virginia Executive Order 51

(Summarized by Joy Hughes)

The order requires us to submit a plan to the governor no later than June 1, 2000 that describes what and when we will be providing current and expanded services to citizens over the Internet. It also requires us to "maximize workstation access to Web-based transactions by agency and institution employees for use in their work assignments and in their status as state employees" Many GMU units have plans to provide current and expanded services over the Internet, which should all be included in the plan. The VP IT will be in touch with the leaders of these groups to include them.

"No later than December 31, 2000, all Executive Branch agencies shall make available over the Internet all forms needed by citizens in interacting with state government." Although this does not mention "institutions," it's wise for GMU to move as far as possible to implementing this order. The VP IT will work with the individual units to assess what forms are required for citizens to interact with the unit and how many of these are currently available over the Internet.

Department of Information Technology (DIT in Richmond) "shall coordinate the efforts of Executive Branch agencies and institutions to leverage the buying power of state government in regard to telecommunications services."

"DIT shall develop policies and procedures regarding access to state databases and data communications in order to ensure the security of such databases from unauthorized use, intrusion or other security threats." (Note: Once DIT develops these policies and procedures, we will need to work together to see that they are implemented at Mason.)

"...privacy best practices by both public and private entities shall be incorporated into DTP's proposed Technology Best Practices Center." It would be wise for GMU to follow the privacy guidelines developed by this group.

…

"The Secretary of Technology...shall review available alternatives and recommend a plan to facilitate the use and authentication of electronic signatures by both the public and private sectors in the Commonwealth. This plan shall be submitted to the Governor no later than November 1, 1999."

"Agencies and institutions shall follow the Secretary of Technology's guidance in incorporating into their proposed plans for Web-enabled government the use of electronic signature technology for both internal and external transactions." GMU will need to follow the state plan in using electronic signatures. The VP IT will survey units to find out if any such projects underway.

Reference:

Executive Order 51: <http://www.state.va.us/governor/eorder/eorder51.htm>

APPENDIX 3. Freedom of Information Act

(Summarized by Jeff Brandwine)

The FOIA applies to all information stored on GMU systems with a very limited set of exceptions. Examples of information not covered by exception include email logs and documents stored in personal directories.

There are approximately 61 exemptions to FOIA -- which would allow the university to have the option as to whether to release requested information. The request must come from a citizen of the Commonwealth of Virginia, and as aside, we do charge the costs of providing copies.

Student records are protected by FERPA -- but can be released via a court ordered subpoena. (We notify the student and student can file a motion to quash the subpoena; if they do not, than we release the information.)

Records within the counseling office would be exempt under medical rules. Much of a personnel record is also exempt -- but salaries, dates of employment, and related items are not exempt.

Furthermore, even if they are exempt under FOIA, we may have to turn records over via a discovery process -- subpoenas -- in litigation involving GMU or even in someone else's litigation.

The University takes every reasonable step to protect and respect privacy; we will, however, turn over documents as required by either state or federal law.

Reference:

<http://www5.infi.net/opengov/opinions.htm>

APPENDIX 4. Computer Security Guide Outline

I. Introduction to Computer Security Basics

1. An introduction to the guide and its purpose.
2. Policies and Guidelines

   This would be a list of links to the current computing policies. (A printed version would contain the full texts.)
3. System Administrator Responsibilities

   This would reference or include the System Administrator requirements (Section 7 of this report) together with a list of the current Administrator "help" groups on campus.

II. Computer System Initial Setup

1. Physical Security

   A list of problems associated with physical security and ways to protect the system.

2 Operating System Security

   This section, customized by OS, would include all of the recommended configurations of security related files plus the location of where to obtain the current recommended "patches" for the system.

3. Backup and Recovery

   How to protect a system's data for restoration in case of major crash or compromise.

4. Account Management

   For "multi-user OSs", how to properly create accounts, check and require the use of "strong passwords" and the use of "permissions" to restrict access to files.

5. Application Configuration

   A list of guidelines, separated by OS, on common applications and how to configure them to provide the best security possible. SSH, SFTP, anonymous FTP, IIS and HTTPd servers are examples of applications that would be included here.

III. Computer Security Tools

1. Access Control

   In addition to built in access control (like IIS has) this would include external programs, like TCP_wrappers, that can enhance security by restricting access.

2. Monitor Systems

   Software like Jammer or Tripwire that will detect "attacks" toward a system or detect changes in the system that may show that someone may have compromised a system.

IV. Computer Security Maintenance

1. Accounting

   Proper use of accounting on multi-user systems.

2. Audit System Logs

   For each OS, how to determine from the standard system logs attempted or successful system probes and compromises. How often and where to look.

3. Security Patch Updates

   For each OS, how, when, and where to look for security updates.

4. Change Control

   Procedures to record changes in system configurations that may affect security.

V. Incident Handling

1. Current GMU Security Issues

   A reference to a "Hot Spots" web page that would describe current compromises that are occurring on campus, quick checks to determine if you have been 'hit' and reminders on where to find patches for these problems.

2. User Incident Handling

   After reviewing the SANS Institute's Step by Step guide, it would appear that this section could be completely covered by purchasing a license to and adopting this guide.

APPENDIX 5. Illustrative Incident Reports

School of Information Technology and Engineering

(1) In early summer 1998, someone broke into the main IT&E server and deleted the accounts and files of numerous users, most of whom were students using the server to store their course work. Many students lost a weeks' work. In the summer session, which has one class meeting daily, this is extremely serious -- that's a quarter of a semester. This causes serious disruption of the summer session, from which a full recovery was not possible.

(2) In January 2000, an IT&E system administrator received a knock on her office door late one Tuesday afternoon. It was the GMU police asking her to help them access a room in which a suspect PC was located. She escorted them to the room and opened it; all the PCs were off. Meanwhile, the Network Manager from UCIS arrived and tracked the IP address to a jack in a different room. In that room, they found a PC on; its the screen indicated that the machine had been used as a pass-through to hack into a company in Idaho. The machine was impounded for over two months while the police investigated. During that time a PhD student could not access the machine to download his research files. This machine will not go back on the network until it has been reformatted and the operating system re-installed. This problem might have been avoided if the student, who was doubling as his own system administrator, knew his responsibilities and kept the PC current with all security patches.

(3) In February 2000, a machine in IT&E was hacked and used to launch a DoS attack on a non-GMU server. Users of the local network began to complain to support@gmu.edu that response time to servers in IT&E was terrible -- e.g., login prompts timed out after 60 sec before all the letters of a password could be typed. The router to which the errant machine was connected was reconfigured to disconnect the machine from the network. The machine, a Sun workstation, was taken off network until it could be cleaned up and recertified. Interestingly, this machine had previously been turned off because its administrator had not installed all the latest security patches. Some system administrators from other labs needed it to test some protocols and turned it on. They forgot to turn it off when done. Within hours, some unknown hacker had found the machine, broke in, and installed a DoS launch package.

Student Dorms

A student writes: One day, I kept getting the message "IP conflict with hardware address xxxxxxxx" every time I attempted to start my computer. The computer would not work -- no Internet, slow local applications. The local applications worked OK if I unplugged from the network. But given that so much of my work is communication with other people, the machine is really useless to me unless it is connected. I called UCIS told them what was going on. They did get

the problem fixed -- four days later. Four days of hell is the way I experienced it. I was very upset.

One of two things could have happened. UCIS could have accidentally reused my IP address somewhere, or a hacker could have hijacked it. Either way, it angered me because I'm so dependent on my computer and Internet connection.

Registrar

(1) Students complained that when they went to the Registrar's office or Financial Aid office, workstations were positioned in such a way as to make their records visible to people in line behind them. After an SRP member brought this to the attention of those offices, the workstations were repositioned so that confidential student information was not visible except to the student and the person helping them.

(2) Students have asked whether information about them in the Registrar's data base is sold outside. The answer is no. This is one of many examples of privacy policies that need to be made more explicit.

(3) A Windows NT Server was compromised in Fall 1999 and used to capture passwords. The compromise was not isolated until January 2000. Academic and administrative user accounts were compromised. The hacker used some of the accounts to launch Denial of Service (DoS) attacks against GMU and non-GMU sites. This affected several groups and network availability both inside and outside GMU -- for example, portions of the GMU network saturated with outgoing packets in the DoS; accounts were unavailable to users, who could not perform their work). At least 80 hours of the time of 15 staff people were consumed to investigate this incident and repair the system.

(4) Some of the DoS attacks mentioned above were directed at GMU systems "pinta" and "mason" using compromised accounts from the Registrar's and Student Accounts office on January 14, 2000. Although the incident itself resulted in very little downtime (several periods of 5 minutes duration), four UCIS security engineers spent a substantial amount of time over the next week to complete the investigation.

(5) On January 31, 2000, two UCIS technicians were dispatched to the Financial Aid office to review Windows NT security on the office's WEB server. Hackers had disfigured the WEB server's home page.

The Institute for Public Policy

(1) TIPP had a number of serious security incidents during 1999. The most significant had to do with the hijacking of one of their "skunk works" servers. This server had been connected to the network without consultation with UCIS, who would have performed a security validation. The machine had no security protection. It was easily compromised. It must have been compromised for a while before we found the problem after other problems started occurring in our

network. We spent over $10,000 on security consultants and several person weeks of staff time figuring out what went wrong and what to do. Eventually, we just had to unplug the server and completely reconfigure it. It was a major hassle for everyone involved.

(2) In another incident, we discovered three accounts that were compromised over two days. It appeared that someone was using a password sniffer to collect passwords of our users. We asked everyone to change both their LAN and OSF1 passwords. UCIS found no sniffer software in any of several suspect machines. We concluded that the sniffer was run from a removable device.

General Mason Systems

(1) A GMU Prince William campus web server was compromised twice in 1998. Because the support staff for the system had neither the time nor the training to maintain security patches, the web pages were moved to GMU's main web server. Recovering from the compromises took about 12 hours total and migrating the web pages took about 80 hours of effort between four individuals.

(2) A GMU Fairfax campus web server was compromised via a vulnerability that the operating system vendor had not yet announced but that the hacker underworld had already discovered. The hacker used the system to run a network sniffer. About 30 hours were used to discover the hack and recover. Additionally, 48 staff-hours were used to reconfigure the system to reduce future compromises. Several web pages were not available for up to 24 hours due to temporary measures initiated to reduce the system exposure. About 6 individuals were impacted.

(3) There are numerous minor security incidents involving compromised user accounts on academic systems. Investigations typically take 1 to 4 hours. The user account is normally disabled until the user reports in person and is given a security lecture and a new password. Normally only the administrator and user are impacted.

(4) In early March 2000, someone hacked “jiju”, the Mason Web Server, through an ISP in the Netherlands. Two UCIS systems engineers dropped everything and spent at least 30 hours investigating the attacks; they closed holes and areas of penetration. In addition, the Mason Web administrator spent time reviewing CGI scripts. Some time of a network engineer was needed to isolate and block the offending IP address. UCIS noticed the attacks because the hacker attempted to execute the “substitute user” command, which is logged. Although no damage was done, the hacker was persistent in attempting to download the password file.

APPENDIX 6. Summary of Recommendations

2. Chief Information Security Officer

2.1.1 Hire a Chief Information Security Officer (CISO) and establish an Information Security Office (ISO) as soon as possible.

3. Risk Assessment

3.1.1 Establish a practice of conducting a campus risk and vulnerability assessment at least once a year. The assessment can be conducted by the Security Review Panel (SRP), which will advise the Chief Information Security Officer.

4. On-Line Electronic Services and Executive Order 51

4.1.1 The VP of IT should issue guidelines for configuring web servers that dispense services and forms for protection and security of data stored there. These guidelines should address

- Configuring interactive web servers for security
- Watermarking pages and forms
- Disclosing privacy policy applicable to each site
- Responsibilities for "record custodians" of each database
- Data gathering, retention, distribution, protection, and ultimate destruction.
- Process for handling objections or grievances regarding the management of private information.

4.1.2 The VP of IT should work with the Provost and Faculty Senate to develop a policy for the process of student evaluation of instruction, given that reports are distributed on-line and data may be gathered on-line.

5. Information Policy Recommendations

Adopt an information policy. A draft is provided.

6. System Recommendations

6.1.1 Almost all the issues listed above could be easily resolved by specifying baseline standards and procedures in a *George Mason University Users Computing Security Guide*. Examples of baseline standards are:

- Rules for safe password selection, frequency of change

- Backup and recovery requirements
- Anti-virus requirements
- Security audit of new installations before attaching to the network
- No shared accounts
- Dormant accounts deactivated after 60 days

We recommend that UCIS create and maintain the *Guide* and that all GMU system administrators be required to use it. Most of the information in the guide would apply to every one of the 16+ operating systems on University computing platforms with some sections customized for different platforms. A basic outline for the Guide is in Appendix 4.

6.1.2 We recommend that a system certification process be developed. The system certification process would be used to verify the security of a system prior to network connectivity being granted. It would be based on a security checklist. The process must define which systems ought to be certified (e.g., personal machines including dialup, laptops, and dorms as well as University equipment). The process must also define what measures, such as disconnection, would apply if a system is compromised.

6.1.3 We recommend that the most sensitive computer systems and databases (e.g., the Student Information System and the Human Resources System) be isolated from the main campus network by firewalls that restrict access and use strong authentication before granting access. UCIS should provide a means by which sensitive databases maintained by any organizational unit can be similarly protected.

6.2.1 We recommend that a new structure for coordinating system administrators be instituted. The new system should include an intermediate level "area coordinators" who know how to contact restrict groups of system "owners". This might be accomplished by adding "Building Coordinators" to the existing 'Telecommunications Coordinators" and developing a hierarchy of support for locating and fixing problem systems.

6.2.2 We recommend the creation of a new database for identifying the assignment of IP addresses. Each record in this database would include:

> Permanent IP address, Hardware address, Type of machine, OS loaded, Location of machine, Owner of machine, System Administration, Department Coordinator, Building Coordinator, Serial # / Property #, a description of what the machine is used for, and system status.

This new system would be linked with the HRS system to update the user information when staff leaves. The system should also include an automatic yearly "renewal" of the IP address allocations to make sure that allocated addresses are still in use.

This same system could / should also be used to fill the existing need for both inventory and seat management that is required by UCIS. At a

minimum, there should only be one database that the others can be extracted from.

6.3.1 Aquire a system (hardware and software) to proactively "scan" all devices on the network to locate and identify known security vulnerabilities. This will NOT be a replacement for proper System Administration. It is intended as an early-warning system for system administrators to help them confirm that their systems are properly administered and to locate systems requiring immediate attention.

6.3.2 Acquire an intrusion detection system. This type of monitor is most likely to be useful if deployed at the Internet gateway, between campus routers and on selected networks (such as dorms, dialup, or Thompson Computer room). (We estimate that the initial cost of a combined intrusion and vulnerability detection system is $125,000 and the annual maintenance cost is $20,000.)

6.3.3 Establish a "red team" reporting directly to the CISO; their job is to probe systems for vulnerabilities and report them with recommendations on how to eliminate them to system administrators.

6.3.4 For each of the measures recommended above -- scanning probes, intrusion detection, and red teams, develop guidelines for the use of the tools, reporting of results, notifying system administrators, and the personal ethical conduct of people who operate the tools or serve on red teams. Define levels of severity of vulnerabilities (minor, severe, critical) and grace periods for correcting them before a vulnerable system will be disconnected from the network.

6.3.5 Establish a process of change management: document deficiencies, risks, and solutions in a database shared by all system administrators. This system can detect if reconfigurations or installations have changed base settings and have created unacceptable vulnerabilities.

6.3.6 Develop a student group who implement, evaluate, and improve on custom tools for monitoring compliance with security standards. This would be a good way to involve aspiring system administrators in the protection of our systems and to train them in the professional and ethical standards of system administration.

6.3.7 Create formal guidelines for GMU administrators on handling security violations. As part of this, adopt the forms and procedures listed in the SANS Step by Step guide for incident handling. This administrator's guide will advise on how to assess whether a compromise has occurred, how to identify the source, how to disable the system with the problem, and how and when to reestablish service, and how to respond if criminal activity is suspected. This guide is not the same as the sections of the User's Guide (Appendix 4) on incident handling.

7. People Recommendations

7.3.1. Adopt as a guideline the "Computer Security Incident Handling Step By Step" published by The SANS Institute. A corporate license is available for $1,800 allowing the posting of the document in PDF format on a GMU internal website. These procedures should be augmented to conform to Commonwealth incident reporting requirements.

7.3.2. Adopt as a guideline three Systems Administrator publications from the USENIX Association. The publications are entitled: "Job Descriptions for Systems Administrators, 2nd ed.", "Hiring System Administrators", and "Educating and Training System Administrators: A Survey." These publications are available the USENIX Association for $7.50 each plus postage.

7.3.3. Develop and institute a university wide program to evaluate and certify systems administrators for different levels of authority. Such a program would be directed by the CISO.

7.3.4 Require an annual signed security agreement as a condition for use of GMU systems for the ensuing year.

7.3.5. Engage with the following methods for increasing user awareness of security issues, policies, procedures, their responsibilities, and the consequences of irresponsibility.

A. Conduct information security presentations at new employee orientation in Human Resources.

B. Conduct information security presentations at student orientation sessions and for Resident Assistants (RA).

C. Sponsor System Administration outreach programs.

D. Develop and distribute information security brochures:

- Paper brochures
- On-line security web page
- Posters in student labs
- Articles in the *Broadside* and *Gazette*: rules and regulations; incidents and consequences.
- *Broadside* interviews with GMU security experts on GMU security issues and implications.

8. Authentication Recommendations

8.1.1 We recommend that the VP IT appoint an engineering group to design and develop an enterprise-wide authentication system. The charter for this group should include:

· Survey the current need for authentication, confidentiality and integrity across all users of the Mason network. Develop a matrix that shows the requirements for all major systems on our campuses. Pay

particular attention to interoperability of systems when charting requirements.

- Evaluate competing technologies.
- Determine the implementation issues of each potential solution.
- Recommend a solution that addresses our needs and provides benefits to GMU users.