




National Science Foundation • Office of Inspector General  
4201 Wilson Boulevard, Suite I-1135, Arlington, Virginia 22230

## MEMORANDUM

**Date:** July 31, 2015

**To:** Dale Bell, Director  
Division of Institution and Award Support

Jamie French, Acting Director  
Division of Grants and Agreements

**From:** Dr. Brett M. Baker   
Assistant Inspector General for Audit

**Subject:** *Labor Effort Reporting under the Federal Demonstration Project's Pilot Payroll Certification Program at George Mason University, Report No. 15-1-017*

Attached is the final report of our audit on George Mason University's labor effort reporting under the Federal Demonstration Project's pilot payroll certification program. The report contains two findings on: 1) internal controls over the support for labor charges to NSF awards, and 2) information technology controls over the protection of payroll information. We have included GMU's response as an appendix to the final report.

Please coordinate with our office during the six month resolution period, as specified by OMB Circular A-50, to develop a mutually agreeable resolution of the audit findings. Also, the findings should not be closed until all recommendations have been adequately addressed and the proposed corrective actions have been satisfactorily implemented.

The Offices of Inspector General at NSF and the Department of Health and Human Services are auditing the implementation of pilot payroll certification systems at four universities. Individual reports will be prepared for each audit; then a capstone report will be prepared when all audits are completed to provide overall results and summarize issues identified at all four universities. This report presents the findings at GMU.

We appreciate the assistance from George Mason University officials, staff, and students that was extended to our auditors during this audit. If you have any questions, please contact Louise Nelson, Director of Audit Services, at (303) 844-4689.

Attachment

cc:	France A. Córdova	Richard Buckius
	Ruth David	Michael Van Woert
	Larry Rudolph	Ann Bushmiller
	Karen Tiplady	Christina Sarris
	Allison Lerner	Fae Korsmo
	Alex Wynnyk	Rochelle Ray
	Louise Nelson	Laura Rainey

**Labor Effort Reporting under the Federal  
Demonstration Project's Pilot Payroll Certification  
Program at George Mason University**

**National Science Foundation  
Office of Inspector General**

**Date  
OIG 15-1-017**



TM 13-E-1-005

---

## Table of Contents

---

Introduction.....	1
Background .....	2
Audit Results.....	5
Findings	
1. GMU Needs to Strengthen its Internal Controls to Ensure Labor Charges to NSF Awards are Adequately Supported.....	5
2. GMU Needs to Strengthen its Information Technology Controls to Protect Payroll Information .....	8
Conclusion.....	9
Recommendations.....	10
Summary of Awardee Response and OIG Comments.....	10
OIG Contact and Staff Acknowledgements.....	11
Appendices	
A. Agency’s Response to Draft Report.....	12
B. Audit Objectives, Scope, and Methodology.....	16
C. Details on Sample Transactions in Error.....	18
D. Sample Design, Methodology, and Results.....	20
E. Additional Details on Information Technology General Controls.....	26

---

## **Introduction**

---

### **Federal Demonstration Partnership (FDP)**

The FDP began in 1986 as an experiment between five Federal agencies (National Science Foundation, National Institutes of Health, Office of Naval Research, Department of Energy, and US Department of Agriculture), the Florida State University System and the University of Miami to test and evaluate a grant mechanism utilizing a standardized and simplified set of terms and conditions across all participating agencies. The result of the test was the establishment of “expanded authorities” throughout the nation, intended to reduce administrative tasks for both the Federal government and research institutions.

One way in which the FDP wanted to reduce administrative tasks involves changing the amount and type of documentation required to support salary and wage charges to Federal awards. Historically, effort reports have been used as the main support for salary and wage charges to federal grants and contracts. Effort reporting is a person-based methodology that allocates each individual’s salary to the various projects he/she worked on during the reporting period. FDP proposes a payroll certification system as an alternative to effort reporting. Payroll certification is a project-based methodology that relies on a project’s principal investigator to certify that all salaries charged to the project are fair and reasonable in relation to the work performed. FDP asserts the alternative is preferable because:

- effort is difficult to measure;
- effort reports provide limited internal control; and
- effort reporting systems may be expensive to implement and maintain.

### **Audits of the Pilot Payroll Certification Systems**

As agreed to by the Office of Management and Budget (OMB), the Offices of Inspector General at NSF and the Department of Health and Human Services (HHS) are auditing the implementation of pilot payroll certification systems at four universities: University of California - Irvine; University of California - Riverside; Michigan Technological University; and George Mason University (GMU). HHS OIG is conducting the audits of the two University of California institutions, while NSF OIG is responsible for the audits at Michigan Technological University and GMU. Although the audit plan and methodology was consistent across all pilot institutions, the results will differ depending on each institution’s implementation of its respective pilot system as well as the nature of the grants and related guidance from the awarding agency (NSF and HHS). A capstone report will be prepared when all audits are completed to provide overall results and summarize issues identified at all four universities.

This report presents the results of the audit work conducted at George Mason University for its NSF awards.

---

## **Background**

---

Our audit scope spanned labor charges at George Mason under both the effort reporting system and the pilot payroll certification process. Therefore, we first developed an understanding of both systems, as implemented by GMU.

### ***Effort Reporting System***

The effort reporting process at GMU began with entering each salaried employee in the payroll allocation system using an appointment letter showing the salary level and award account to be charged. This award information, along with knowledge of all other employee workload cost categories, was used to establish the percentage of effort in the payroll allocation system for all activities planned for the employee. This planned allocation of effort for each staff person is entered into the Banner payroll allocation system, and the total allocation must equal 100 percent.

The planned distribution of effort may be amended during the semester, or between semesters, as needed, for changes in workload effort or changes in projects/activities. Such changes are made using a fund change request form. However, because of the nature of the NSF grants, the researchers (frequently graduate students) typically only work on one award at a time, so their effort was not often distributed across multiple awards or activities at the university. In fact, of the 499 employees who charged salaries to NSF during our audit period, 390 (78 percent) allocated full salaries (on a pay period basis) to a single NSF project account rather than to multiple projects.

At the end of each semester, a printout of each employee's distribution of effort (referred to as a Personnel Effort Report) is system-generated and signed by either the employee, or someone with first-hand knowledge of the employee's effort, to certify that the labor distribution supporting the award charges is "reasonable in relation to the work performed" during the semester. For all salaried employees—faculty and graduate students—individual timesheets were not required. However, per GMU policy, PIs are responsible for approving the certifications of graduate students. As faculty and graduate students account for 94 percent of the labor effort charges to GMU's NSF awards, the vast majority of salary charges were not supported by biweekly timesheets, but rather by effort reports certified on a semester basis. Biweekly timesheets signed by the employee were only required for hourly employees—undergraduates and all non-faculty staff—and accounted for just six percent of labor charges. Therefore, for the majority of the payroll charges, traceability back to a specific daily or biweekly activity report is not possible, nor is it required by OMB Circular A-21.

### ***Pilot System***

George Mason's process for initiating research salary charges was the same under the pilot as under the prior effort reporting process, as depicted in the following chart. The difference is that GMU's annual certifications (Sponsored Project Payroll Expense Reports, or SPPERs) included individual salaries (dollar amount and percentage) charged to the respective awards for all employees who worked on the project during the reporting year. The PI is solely responsible for

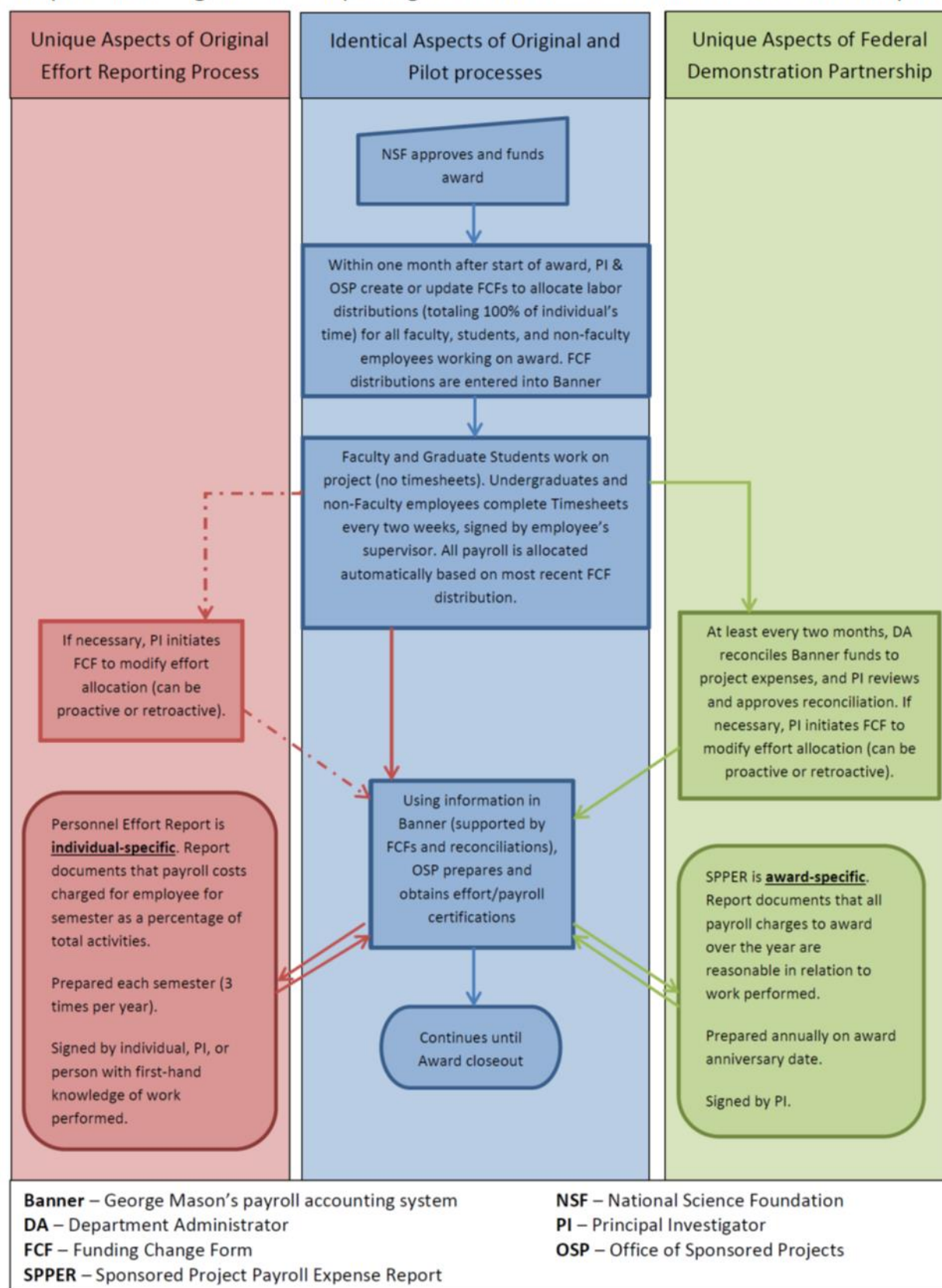
certifying annually that salary and wage expenses are “reasonable in relation to the work performed” for all employees included on the report. This certification meets the requirements stated in the FDP pilot as well as OMB Circular A-21 requirements under a “Plan-Confirmation” method of payroll distribution. The certification is to be completed and returned to the Sponsored Project’s Office within 120 days from the end of the annual certification period or, per GMU policy, the university will transfer the costs out of the sponsored project account. However, the certification does not report effort on other awards the individual worked on during the reporting period, which is a risk.

An additional control in the pilot process that is not part of the prior effort reporting process is a requirement for bimonthly reconciliations of award ledger and expense data. The department administration performs the reconciliations and certifies that all charges and credits to the fund or organization have been reviewed and are supported by appropriate documentation. GMU policy also provides for PI review and approval of the charges but does not require this review to be documented by the PI. These periodic reconciliations, if properly performed, provide a level of control that did not exist under the prior effort reporting system.

### ***Comparison of the Previous and Pilot Processes at GMU***

The following flowchart depicts the similarities and differences between the two processes at GMU. Both the prior effort reporting process and the pilot payroll certification process utilize payroll information maintained in the Banner system.

## Comparison of Original Effort Reporting Process to Federal Demonstration Partnership Pilot





---

## **Audit Results**

---

We performed this audit to determine whether GMU's payroll certification system provided accountability over federal funds. An area of particular concern was whether the pilot system's shift away from certifying 100 percent of individual employees' efforts put federal funds at an increased risk of improper allocation. We based our determination on assessments of GMU's controls designed to (1) ensure that the university charged allowable labor costs to its NSF awards and (2) secure the data used to support labor charges.

To test the controls over the allowability of labor charges to NSF awards, we selected a sample of 180 payroll transactions for review. Our sample included transactions under both GMU's payroll certification pilot and the prior effort reporting system. While many of the steps under the pilot were unchanged from the prior system, several were different, as discussed in this report. Overall, we found that GMU did not always comply with its documentation policies for payroll transactions under the payroll certification pilot.

We also identified weaknesses in the controls over Banner, the system GMU uses for payroll allocation, under both the effort reporting system and the payroll certification pilot. Specifically, the university did not use two-factor authentication to access Banner; did not adequately manage access controls; did not install security patches in a timely manner; and did not update its risk assessment for Banner. As a result, the data retained in the Banner information system to support payroll charges to federal awards may not be secure and could be vulnerable to access by unauthorized users who could modify information.

---

### **1. GMU Needs to Strengthen its Internal Controls to Ensure Labor Charges to NSF Awards are Adequately Supported**

---

George Mason requires the following documentation as support for labor charges to federal awards: timesheets for hourly employees; appointment and/or tenure letters for faculty working on federal awards; appointment letters for students and non-faculty working on federal awards; funding change forms for payroll allocation initiation and changes; semester certification of work performed (effort reporting only); bimonthly reconciliation of budgeted expenses to actual project expenditures (pilot only); and annual certification of payroll expenses charged to each federal award—SPPERs (pilot only). Based on the type of transaction that was tested (initial labor charge or labor cost transfer), at least one of these documents was required to support a specific sampled transaction. To test the effectiveness of GMU's internal controls over both payroll allocation systems, we selected a sample of 180 transactions,<sup>1</sup> representing \$209,195 of costs charged to NSF awards, from a universe of 9,676 transactions, representing \$11,914,994 in NSF payroll charges. The transaction universe included one year under the prior effort reporting process (January 2, 2010, through December 31, 2010) and more than two years under the payroll certification pilot (January 1, 2011, through March 31, 2013). We were particularly interested in the accuracy and timeliness of GMU's labor certifications, as required by institution policy.

---

<sup>1</sup> See Appendix D for the sample design, methodology and results.

We found problems (which are detailed below) in 21 of the 180 sample transactions we tested, totaling \$23,385. Another transaction, for \$107, was an incorrect posting to a payroll account for a relocation benefit. GMU reversed the relocation charge after we brought the error to the university's attention.<sup>2</sup>

If the inaccuracies and lack of adequate supporting documentation found in the sampled transactions occurred with the same frequency across the population, we project that GMU lacked adequate supporting documentation for \$709,064 out of the \$11,914,994 salary costs claimed against NSF awards during the audit period. Fringe benefits and facilities and administrative (F&A) costs associated with the projected costs are [REDACTED] and [REDACTED] respectively. Our estimate was based on a universe of 11,347 total payroll transactions<sup>3</sup> projecting the identified errors at 90 percent confidence.<sup>4</sup> The majority of the problematic transactions were the result of GMU failing to follow its own internal policies and procedures.

The following sections describe the documentation issues identified in our audit.

### Timeliness of Certifications

Under the payroll certification pilot, GMU policy requires PIs to review and certify SPPERs and return the signed form to the Office of Sponsored Programs. If the expense report has not been returned to that office within 120 days after the end of the reporting period, GMU policy states that the university will transfer the costs out of the sponsored project account.

Our sample of 180 transactions included 94 transactions under the payroll certification pilot that required certification on 60 distinct SPPERs<sup>5</sup>. We found that 11 SPPERs (representing 19 transactions in our sample) were not certified in a timely manner. The average number of days certifications were late was 224, with one report certified 706 days late and four others more than 300 days late. Although GMU's policy required it to transfer costs certified more than 120 days late from the sponsored project, we did not find any instances when the university credited NSF for costs charged in violation of its own policy.

Our sample included 32 transactions under the prior effort reporting system, requiring certification by semester on 30 effort reports. We did not identify any late or missing effort certifications in these transactions.

---

<sup>2</sup> See Appendix C for details on sample transactions in error.

<sup>3</sup> GMU's total payroll transaction universe during the audit period included 11,347 transactions. We excluded transactions of \$100 or less as candidates for selection in our sample, leaving a total of 9,676 from which the sample of 180 transactions was drawn. (See Appendix D)

<sup>4</sup> See Appendix D for complete details of the sample design, methodology, and results.

<sup>5</sup> SPPERs cover multiple employees over an entire year, so one certification/SPPER includes numerous payroll transactions.

### Funding Change Forms

Funding change forms were used in both the effort reporting process and in the pilot to make changes during the course of a project. We found one error on the 14 funding change forms we reviewed that fell under the effort reporting system. The error (\$276) occurred because GMU transferred funds from a non-sponsored account onto an NSF award account in order to expend the available funding under the award. GMU provided no support that the charge involved actual work performed on the award.

We did not find any errors involving funding change forms from the 41 we reviewed for the payroll certification pilot.

### Timesheets

Under both the effort reporting and pilot payroll certification systems, GMU required hourly employees to complete biweekly timesheets that need to be approved by the project PI. Our sample transactions included 53 transactions supported by 52 timesheets for 20 employees. All timesheets in our sample were submitted and approved as required under both systems. However, in reviewing the documentation, we noted one instance (\$156) under the effort reporting system where GMU failed to follow its internal policy to obtain prior approval to allow a student to work on both a graduate position and a student wage position within the same period.

### Bimonthly Cost Reconciliation

In 2013, an internal audit at George Mason University found that bimonthly reconciliations were not always reviewed and approved as required. Our review of 14 bimonthly reconciliations under the payroll certification system found only two that were completed correctly. Of the remaining 12, nine were not signed by both the preparer and the approver, two were certified late, and one was certified prior to the end of the reporting period. As a result of these problems, the university lacked assurance that ongoing expenditures under the pilot payroll certification system were being made for the intended purpose. This interim control is critical to assuring that the annual certifications are accurate.

As stated above, a primary concern of this audit was to determine whether the fact the pilot system does not require certifying 100 percent of each employee's effort increased the risk of improper allocations of payroll. We found that full allocations remain recorded and available within GMU's systems. Nonetheless, when PIs certify the salaries charged to their awards, they do not have records of full payroll allocations for employees who worked on their projects. Visibility over full payroll allocations provides greater assurance that project costs are accurate. Therefore, making full allocations available to PIs would be useful in assuring payroll charges to federal awards are accurate. Additionally, accounting for full allocations of employees' time could be an important control to help ensure that overcharges and inaccurate charges do not occur.

Based on the number and types of errors we identified from the transaction testing, GMU needs to strengthen enforcement of its internal controls over its payroll allocation and certification processes to ensure labor charges to NSF awards are adequately supported, as required by federal regulation and NSF and university policy. The most prevalent issue we found in examining payroll transactions was late certification of SPPERs under the pilot system. When reports are certified months, and in some cases years, after the work is done, it puts the reliability and accuracy of the supporting documentation at risk. In addition, the late certifications resulted in GMU not having timely support for payroll expenses for which it had already been reimbursed.

We also found that GMU was not completing bimonthly reconciliations timely. Because the bimonthly reconciliations provide interim verifications between the longer timeframe of the annual certifications, timely completion of the interim checks improves confidence in the annual certification of labor charges under the pilot system.

---

## **2. GMU Needs to Strengthen its Information Technology Controls to Protect Payroll Information**

---

Both the prior effort reporting process and the pilot payroll certification process utilize payroll information maintained in the Banner system. Auditors identified the following areas in which IT controls needed to be strengthened:

- GMU did not employ two-factor authentication to access Banner as recommend by National Institute of Standards and Technology Guidance. Two factor authentication provides additional security because the user has to have two means of identification, one of which is typically a physical token, such as a card, and one of which is something that is memorized, such as a security code. GMU officials told us that they are considering alternative controls.
- GMU did not adequately manage access controls as required by university policy. This weakness could permit unauthorized users to obtain or alter sensitive information and gain access to financial records. For example, [REDACTED]  
[REDACTED]. University officials told us that some accounts were created before GMU instituted strong password management and that the accounts have not been accessed since the password controls had been implemented.
- Auditors found that [REDACTED]. Auditors found [REDACTED].  
[REDACTED]. GMU officials told us that they plan to institute a supplemental reconciliation process to ensure that accounts are locked in a timely manner.
- GMU did not install security patches to the Banner Oracle database in a timely manner. Patch management is the process of identifying, reporting, and effectively fixing IT system flaws. Patching in a timely manner helps maintain operational efficiency and

overcome security vulnerabilities. GMU officials told us that patches are applied as soon as possible but are subject to scheduling around Banner, systems and network upgrades.

- GMU did not update the risk assessment for Banner to reflect major architectural changes to the system, as required by university policy. GMU officials stated that GMU updates its risk assessments when one of the following occurs: (1) a new system is implemented; (2) significant changes occur; or (3) every three years.

As a result of these IT control weaknesses, the data in the Banner information system used to support payroll charges to Federal awards may not be secure, and could put the reliability of information used as the basis for labor charges to federal awards at risk. These system weaknesses were identified under the prior effort reporting process and still existed during the pilot process. Therefore, the reliability of the payroll and effort reporting cost data used to support GMU labor charges is at risk until these control weaknesses are addressed.

---

## **Conclusion**

---

Late certifications under the pilot system was the most prevalent issue identified in the transactions sampled. For example, certifications of labor reports we found to be in error were an average of 224 days late. When reports are certified months after work has been completed, there is a higher likelihood that labor will be charged incorrectly. We concluded that these problems occurred because GMU did not follow its internal policies and procedures, and not as a result of inadequate design of pilot system controls. When reviewing the IT controls over the Banner information system, we identified many access and security weaknesses that occurred because GMU failed to establish and enforce adequate controls. Given that the data for both the effort reporting and pilot processes was housed in Banner, these IT weaknesses were not attributable to the design of either the effort report or pilot certification systems but rather to GMU's management of the Banner system as a whole.

Both the pilot system and the prior effort system rely on the people and systems involved and on the institution to have adequate internal controls to ensure that its policies and procedures are followed. If institutions use the pilot, they need to ensure that they have strong internal controls to ensure the payroll charges are adequately supported. If schools are going to certify the documentation less frequently, they have to be more diligent in ensuring that the control procedures are communicated and adhered to on a consistent basis. Additionally, maintaining the full allocation of payroll to each individual's activities is important to ultimately ensure adequate support for Federal labor charges. Having direct visibility of each employee's full payroll allocation, including percentage allocations assigned to other awards or projects, is important to a PI to ensure the percentage assigned to his or her project is reasonable. Accounting for full allocations of employees' time could be an important control to help ensure that overcharges and inaccurate charges do not occur. There are challenges with any payroll allocation system, and strong internal controls are the key to ensuring taxpayer funds are appropriately charged and adequately protected from misuse and abuse.

---

## Recommendations

---

We recommended that NSF's Director of the Division of Institutional and Award Support (DIAS) direct George Mason University to:

1. Enforce its written policies for the pilot payroll certification system. Areas needing enforcement include:
  - a. Ensuring that annual SPPERs are completed and returned in a timely manner.
  - b. Ensuring that costs associated with late SPPERs are transferred to non-sponsored accounts.
  - c. Ensuring that bimonthly reconciliations are completed and returned in a timely manner.
2. Enhance internal controls over information technology as follows:
  - a. Implement two-factor authentication for access to Banner.
  - b. Implement controls to ensure that passwords for all GMU accounts meet GMU's revised password requirements. In addition, dormant accounts should be reviewed and locked whenever possible.
  - c. Implement a process to ensure that accounts eligible for closure are locked.
  - d. Implement a process to ensure that Oracle security patches are installed promptly.
  - e. Implement a process to ensure that risk assessments are current and accurate and updated when significant changes occur.

---

## Summary of Awardee Response and OIG Comments

---

GMU officials generally agreed with the findings and recommendations, and acknowledged that institutions under payroll certification systems must have strong internal controls to ensure payroll charges are adequately supported.

Regarding the timeliness of certifications, GMU stated that since the timing of report generation may vary based on a variety of factors, the policy related to removing charges has been based on the time a PI has to certify a report once received (60 days from the distribution date). Although GMU was able to identify and explain the late certifications identified in our report, the written policy specifies 120 days from the end of the award year to complete the certification. Therefore, the audit findings remained as originally written. GMU agreed that in order to ensure there is a clear understanding of the policy and there are not unnecessary delays, it will update the policy to clarify language regarding removing costs and when certifications will be generated and distributed. It also agreed that bimonthly reconciliations are a critical control step, and stated that it is developing improved reconciliation reports and will continue outreach and training on this critical step in the process.

Regarding the information technology recommendations, GMU responded that it has initiated a formal project to assess the use of two-factor authentication, and stated that it has improved several controls related to account management. However, GMU disagreed with a statement regarding Banner data vulnerability and the associated risks. As stated in our report, the Government Accountability Organization (GAO) has long recognized the importance of patch

management to minimize system vulnerabilities. The audit found that some security patches were not installed in a timely manner, which constitutes a risk, and therefore our finding was not changed.

See Appendix A for the full text of GMU's response to the draft report.

---

## **OIG Contact and Staff Acknowledgements**

---

Louise Nelson, Director, Audit Services  
303-844-4689 or [lnelson@nsf.gov](mailto:lnelson@nsf.gov)

In addition to Ms. Nelson, Laura Rainey, Daniel Buchtel, Darrell Drake, Brittany Moon, Keith Nackerud, Jeremy Hall, and Jennifer Miller made key contributions to this report.

---

## Appendix A: Auditee Response to Draft Report

---



June 29, 2015

Re: George Mason University Response to Draft Audit Report

Dear Ms. Nelson:

Thank you for the opportunity to review and respond to the National Science Foundation (NSF) draft report titled, "Labor Effort Reporting under the Federal Demonstration Project's Pilot Payroll Certification Program at George Mason University".

George Mason University (Mason) has been a member of the Federal Demonstration Partnership (FDP) since 2008 and is committed to the FDP's mission to improve productivity of research without compromising its stewardship of federal funds. As one of the four Pilot Schools participating in the Payroll Certification Pilot, Mason has been pleased to not only meet the conditions outlined in the Pilot, but continually look for opportunities to refine processes and procedures to ensure that the goals of the pilot were achieved. We feel we have improved Principal Investigator (PI) oversight of direct salary/wage charges to federal awards by simplifying the salary certification process for federal awards while significantly reducing administrative burden and allowing PIs to spend more time on research. Since implementing Payroll Certification at Mason in January 2011, we have identified opportunities to strengthen controls related to salary charges on federal awards throughout the labor distribution process. We agree with the NSF OIG that under payroll certification, institutions must have strong internal controls to ensure payroll charges are adequately supported.

### Timeliness of Certifications

The draft report indicates the Mason Payroll Certification policy requires payroll certification reports to be returned to the Office of Sponsored Programs (OSP) within 120 days from the end of the period or costs will be transferred from the sponsored project account. Since the timing of report generation may vary based on a variety of factors, the policy related to removing charges has always been based on the time a PI has to certify a report once received (60 days from the distribution date). This aspect of the policy is reinforced in training materials and the email used to distribute payroll certification reports each month. Mason's Payroll Certification Policy indicates that payroll certification reports will be returned to the Office of Sponsored Programs (OSP) within 60 days of distribution or the associated



costs will be removed to a non-sponsored source of funding. Since implementing payroll certification in January 2011, all reports have been returned within 60 days of distribution.

One aspect of the pilot that has been adjusted and improved is related to the date parameters used to generate payroll certification reports. Initially, the end date was being used, but we identified issues with partial year extensions and early closeouts that made it clear that using the start date to generate reports would be preferred. On Appendix C of the draft report SPPERs 1 – 5 are attributed to procedural reliance on award end date that was changed to award start date when the problem was identified. The payroll certification program encountered an unexpected error when a project report was produced with a PI name over the maximum limit of 25 characters. When the error was discovered by management the defect was identified and corrected, the report was distributed and returned timely. On Appendix C of the draft report SPPER 6 is attributed to this issue.

During the winter break the University formally closes with all academic and business offices formally closed. This is typically an extended period 10-14 days depending on the calendar. On Appendix C of the draft report SPPERs 7, 8, 9 and 11 are attributed to slight delays related to University closing.

The report generation may vary by month based on the calendar, timing of the month end closing, workload and other factors. On Appendix C of the draft report SPPER 10 was distributed after the close of the prior month and was certified and returned to OSP within 60 days of distribution.

In order to ensure there is a clear understanding of the policy and there are not unnecessary delays, Mason will update the policy to clarify language about removing costs and that payroll certification reports will be generated and distributed by OSP no later than 15 days after the end of the period.

#### Bimonthly Cost Reconciliation

Mason concurs that bimonthly reconciliations are a critical control step and it is important to ensure they are completed and returned in a timely manner. We are developing improved reconciliation reports and will continue to provide outreach and training to all individuals responsible for reconciliation to ensure this step is completed in a timely manner.

#### Information Technology

Information Technology Services (ITS) at Mason continues to assess and respond to the needs of the university and, specifically, the increasing demands and risks associated with IT security. A new Chief Information Officer (CIO) was appointed in December 2013. After feedback from many university departments, the CIO reorganized the ITS in February 2015, changing the name from Information Technology Unit to IT Services to emphasize that its purpose is to provide services to meet all customers' needs. The CIO also formed an Information Technology Governance Group (ITGG) which reviews all IT projects and prioritizes them so that ITS will better understand the university's goals. The ITGG provides a forum for transparency, and for departments to express needs and seek support. The IT

Security Office (ITSO) has engaged in such projects as implementation of an IT Risk Management System, expanding and updating the Security Information Event Management (SIEM) and the Vulnerability Detection Systems, and PCI DSS compliance. Mason concurs with the NSF OIG assessment that there were areas in which it needed to strengthen its information technology controls to protect payroll information.

As a result, Mason initiated a formal project to assess requirements and select a two factor authentication solution for privileged access. As a result, a formal pilot project is being conducted where Systems Engineers will use two factor authentication to log into servers. After gathering information from the pilot, Mason will expand the two factor authentication to Internet Native Banner users. The program will expand to more Banner users in the near future.

Mason has implemented the following controls for account management:

Daily review of the job change report for job status. Accounts of questionable status are locked. Supervisor approval is required to unlock these accounts.

Review of accounts on Thuban for inactivity is conducted every 180 days. Inactive accounts are disabled. Users are required to go through the Banner Accounts request process defined by Banner governance to have accounts re-enabled.

Required Oracle accounts for all Mason Staff are created in a locked status. Passwords for these accounts expire after 180 days if they have not been changed.

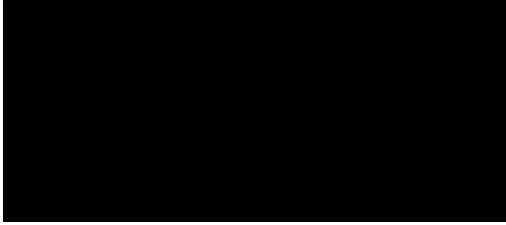
For Banner Oracle accounts the Database Verify function is used to force password expiration and account locking for passwords that have not been changed for 180 days. Supervisor approval is required to unlock these accounts. Account owners must then reset their password using Mason's password change site that enforces strong password policy.

Standard Operation Procedures have been created to govern the above controls.

Mason does not believe that, "Banner data could be vulnerable to exploits that could lead to unauthorized access or denial of service to critical entry points into the IHS network" because there is no business relationship between Banner and IHS nor a particular network configuration that would allow for this. However, a Standard Operating Procedure (SOP) has been written requiring the application of Oracle critical patches on a timely, regular schedule. The SOP specifies the Request for Change (RFC) process to include the specific patches that will be applied. Only an emergency exception defined by our change management policy may delay a scheduled patch. Patching will occur at the first maintenance window after this exception. In addition, RFCs occur every three months within three months of the release of each Oracle critical patch.

Risk assessments for Banner are current as of April, 2015.

Sincerely,



---

## **Appendix B: Audit Objective, Scope and Methodology**

---

The objective of the audit was to determine whether George Mason University's (GMU) payroll certification system provided accountability over federal funds. An area of particular concern was whether the pilot system's shift away from certifying 100 percent of individual employees' efforts put federal funds at an increased risk of improper allocation. We based our determination on assessments of GMU's controls designed to (1) ensure that the university charged allowable labor costs to its NSF awards and (2) secure the data used to support labor charges.

The payroll certification pilot started at GMU in January 2011. The audit was announced on March 11, 2013. The audit scope encompassed the period of January 2, 2010 through March 31, 2013. We selected 180 of 9,676 transactions to test, totaling \$209,194 of the \$11,914,994 sample universe. See Appendix D for the sampling design, methodology and results.

We gained an understanding of the payroll certification processes (both the pilot and the former processes used at GMU); payroll processes; how these processes relate to both the labor costs in GMU's general ledger, and how labor costs are charged to Federally sponsored awards. We also performed on-site visits to obtain an understanding of the processes, procedures, and internal controls related to the scope and objectives of the audit. Our focus was on the labor certification process, labor effort recording and reporting, and accountability for labor costs charged to NSF awards.

In order to ensure that we have a comprehensive universe of all payroll related transactions charged to Federal awards by GMU, we obtained reconciliations between the General Ledger (GL) and the payroll subsidiary ledger; between the payroll subsidiary ledger and the payroll certification records; and also between the payroll sub ledger, payroll certification records and the GL; and, between the GL and the Federal Financial Reports (FFR). We requested and analyzed all pertinent GL, Payroll Subsidiary Ledger, and labor effort details (timesheets, appointment letters) and performed data analytics to target payroll-related transactions for detailed test work.

We utilized data analytics to establish business rules that were utilized for risk assessment of the data and also to formulate strata. Under the data analytics process, 100% of all labor-related transactions were subject to review utilizing the business rules developed to test the transactions.

We relied on the work of an HHS OIG statistical specialist, who used the HHS OIG Office of Audit Sampling Policies and Procedures and RATSTAT to stratify the data and select a simple random sample from each stratum for testing. We also relied on the work of an HHS OIG IT auditor to conduct the IT portion of the audit.

For each employee for which a transaction was selected for review, we obtained and reviewed supporting documentation to determine whether labor costs were actually incurred, benefited NSF awards, and were accurately and timely recorded and charged to NSF awards. We also conducted on-site interviews of selected employees to obtain corroborating evidence of the documentation.

We tested the 180 sample transactions for allowability against the following criteria:

- Generally Accepted Accounting Principles (GAAP)
- National Institute of Standards and Technology guidance on information technology
- OMB Circular A-21, Cost Principles for Educational Institutions
- NSF Proposal and Award Policies and Procedures Guide (PAPPG)
- Individual award agreements
- GMU Policies and Procedures

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

We held an exit conference with George Mason University officials on April 21, 2015.

## Appendix C: Details on Sample Transactions in Error

### Late Labor Certifications

19 sample transactions, totaling \$22,958, were documented by late certifications. The following table summarizes these charges:

SPPER	SPPER Total	Sample #	Sample Amount	NSF Award #	GMU Fund #	EOP	EOP + 120 Days	Date Returned	# Days Late
1	4,226.65	55	845.33	██████	202224	07/31/2011	11/29/2011	11/04/2013	706
2	32,390.25	125	4,296.75	██████	200982	08/31/2011	12/29/2011	11/05/2013	677
3	24,666.70	155	555.56	██████	201316	08/31/2012	12/29/2012	11/05/2013	310
4	50,529.61	147	2,310.99	██████	201865	08/31/2012	12/29/2012	11/04/2013	310
5	46,427.96	144	160.55	██████	20005A	08/31/2012	12/29/2012	No Date Stamp (certified 11/01/2013)	309*
6	31,117.97	159	875.00	██████	202470	09/30/2012	01/28/2013	04/01/2013	63
7	122,388.22	102	940.84	██████	202172	08/31/2011	12/29/2011	01/26/2012	28
		110	1,747.22						
8	132,149.37	35	2,363.89	██████	201861	08/31/2011	12/29/2011	01/26/2012	28
		83	762.56						
		111	762.56						
9	161,782.37	37	2,130.19	██████	202172	08/31/2012	12/29/2012	No Date Stamp (certified 01/18/2013)	22*
		38	522.41						
		39	522.41						
		143	857.14						
10	30,463.21	44	1,260.42	██████	202340	06/30/2013	10/28/2013	11/04/2013	7
		47	1,027.74						
11	28,137.00	179	800.00	██████	201880	08/31/2013	12/29/2013	No Date Stamp (certified 01/03/2014)	7
<b>Totals</b>	<b>664,279.31</b>		<b>22,952.97</b>					Average:	<b>224.3</b>
* = 2 days added to certified date for calculation of lateness									

### Funding Change Forms and Lack of Prior Approval

We found two transactions, totaling \$432, for which GMU failed to follow institution policies and procedures:

One sample transaction (#59) of \$276.49 was part of a transfer of \$480 from a non-sponsored account to NSF award # ██████ just prior to the June 30, 2010, expiration of the NSF award. The Funding Change Form, dated June 11, 2010, and applicable to the academic year ending May 24, 2010, stated, “includes \$480 available from the grant” and that “additional work was performed during the AY [Academic Year] to justify the additional \$480 in funding from the grant.” Given the timing and amounts involved in the transfer, it appears that costs were transferred onto an expiring award in order to draw down the remaining balance. In addition, there was a lack of segregation of duties. The employee identified on the cost transfer was also

the PI for the award. However, only the then-Business Manager for the School signed the Funding Change Form, noting “for” in the spaces for signatures of both the PI and the Dean.

One sample transaction (#112) included \$156.00 in wage costs for 12 hours charged to NSF award # [REDACTED] for an employee who held a 20-hour assistantship for another project. There was no prior written approval for the employee to work on the second project while still maintaining the other appointment, as required by GMU policy.

#### Incorrect Relocation Charge

One sample transaction (#54) represented relocation benefits of \$106.99 that were incorrectly charge to NSF as payroll costs. We brought this to GMU’s attention during audit fieldwork. When we brought this error to GMU’s attention, officials agreed that the charge was posted in error and reversed the transaction.

---

## Appendix D: Sample Design, Methodology, and Results

---

We used stratified sampling to select a sample of 180 payroll transactions for testing during the audit. The sample design, methodology, and results are as follows:

---

### Sample Design and Methodology

---

**Population:** The population contained all salary and wage transactions charged by George Mason University (GMU) to its NSF awards for the period January 2, 2010, through March 31, 2013.

**Sampling Frame:** GMU provided two excel files of GMU's accounting system general ledger and payroll sub-ledger for the period January 2, 2010, through March 31, 2013. From these ledgers, we identified 11,347 individual payroll transactions (transaction) records totaling \$10,974,916. The NSF OIG Data Analytics Team (DAT) imported the original excel files into its ACL tool (the ACL Project). After data analytics (see Sample Design, below), we removed all transactions equal to or less than \$100. This included the removal of all negative dollar transactions. This resulted in a sample frame consisting of 9,676 transactions totaling \$11,914,994.

**Sample Unit and Design:** The sample unit was an individual payroll transaction. All transactions within the sampling frame underwent data analytics tests covering four areas of high risk: charges to expired awards, excess salary charges, high risk adjustments, and administrative salaries (e.g., indirect costs) charged directly to awards. Each area of high risk comprised a stratum for statistical sampling purposes. All transactions that did not fall within one of these 4 strata placed in Strata 5 entitled "All Other Transactions." Details of the steps used in the development of the five strata and rules followed in assigning transactions were as follows:

#### Stratum #1 - Charges to Expired<sup>6</sup> Awards

- DAT calculated a field "No of Days Posted After Expiration Date" which finds the number of days after an award expiration date that the salary amount was posted to GMU's payroll sub ledger.
- DAT calculated the number of days after the award expiration date the employee performed the work.

#### Stratum #2 - Excess Salary

2-month Salary Limit: DAT conducted the 2 month salary limit for senior NSF project personnel as follows:

---

<sup>6</sup> Note: In calculating award end dates, DAT considered any with-cost and no-cost extensions to GMU's awards.



- DAT sent to GMU a list of employees determined to be Senior Personnel Account Codes (pursuant to GMU definitions). GMU provided the appointment type and salary amount for each employee on this list.
- GMU data was used to determine the “2 Month Limit Amount” calculation for each employee. Based on limitations within the GMU data, DAT developed a conservative decision rule wherein the rate used to calculate the 2 Month Limit Amount was the highest base salary amount for each employee's permanent position.
- For 12-month faculty, the effective date of the appointment year used for the calculation was July 25th; for 9-month faculty, the effective date used was August 25th. We also assumed a 9-month appointment for faculty for which there was no identifiable appointment. For the purposes of data analytics, the same year was used for a 9-month appointment as a 12-month appointment.

High Risk Pay Transactions: DAT identified Account Codes [REDACTED] and [REDACTED] which are defined as follows, as high-risk:

- [REDACTED] Classified Annual Leave Balance
- [REDACTED] Relocation Benefits Taxable
- [REDACTED] Relocation Benefits Non-Taxable
- [REDACTED] Overtime-Wages

Graduate Research Assistant (GRA) Exceeds Hours: According to GMU Policy, student employees are students first and foremost and, in recognition of this, should be limited to a total of half-time employment each month. During semester breaks, students may be employed full-time. The GMU policy specifically states that prior approval is required for GRAs to work over 20 hours per week.

DAT conducted data analytics to determine if student salary payments complied with the GMU policy. GMU policy also indicates that Full-Time Graduate Research Assistantships consist of 20 hours per week (or more with prior approval) and Part-Time Graduate Research Assistantships are less than 20 hours per week (commonly 10 hours per week).

In reviewing the data, DAT determined for the characteristic of interest (e.g., student payments outside the GMU policy): 43.33 and 86.67 hours were used rather than 40 and 80 hours because all of the graduate students are paid semi-monthly (analytics was performed based on a semi-monthly appointment).

The data was also reviewed for possible overpayments to GMU employees as follows: A full time employee that is paid semi-monthly works 86.67 (2080 hours/24 pay periods) hours per pay period and 43.3 hours if they work half time.

### Stratum #3 - High Risk Adjustments<sup>7</sup>

---

<sup>7</sup> All intra-award adjustments were eliminated from the results as they were deemed low risk. An adjustment is identified as an intra-award adjustment if it is posted to the same award on the same day and under the same document code.

DAT defined high risk adjustments using auditor and data analyst judgment after gaining an understanding of the types of adjustments within the GMU data, by reviewing GMU policy and Procedures, and by reviewing patterns within the data for adjustments. We determined that the Following Pay Event Type Indicators to be high risk adjustments:

- I (Reissue)
- J (Adjustment)
- M (Manual)
- R (Redistribution)
- V (Void)

#### Stratum #4 - Administrative Salaries

DAT summarized the payroll sub ledger GMU as follows:

- (a) Account Code;
- (b) Job classification code - job title; and,
- (c) Job employee classification - appointment type.

We identified all codes that appear to include charges to administrative type salaries. The criteria used to define administrative type salaries included NSF grant policy guidance, the OMB Circulars, and descriptions of account codes, The following codes were designated as administrative type salaries are included in Stratum 4:

- (a) Account code: [REDACTED] (Faculty Salary Administrative)
- (b) Job title: 00070Z Police Officer  
02332Z Office Manager/Project Manager)  
09105Z Police Sgt.  
10373Z Business Manager  
FA01AZ Associate Dean Student Affairs  
FA052Z Interim VP University Relations  
FA14AZ Coordinator Governor's School  
FA934Z Director Emergency Management Fire Services  
WG8071 Nonstudent Wage, GMU Worker
- (c) Appointment Type: FA, PS

#### Stratum #5 - All Other Transactions

Any salary and wage transactions that did not fall within any of the other strata were placed within Stratum 5.

To ensure that all transactions were unduplicated, appearing in only one stratum and only once in the sampling frame, a hierarchy was established for assigning transactions to a stratum. We assigned transactions that shared the attributes of multiple high risk categories to just one category based on the following hierarchy: Charges to Expired Awards, then Excess Salary, then High Risk Adjustments, then Administrative Salaries and lastly All Other Transactions.

The application of criteria to the various stratum resulted in the following sampling frame:

<b>George Mason University</b>			
<b>Stratum</b>	<b>Record Count</b>	<b>Dollar Value</b>	<b>Number of Sample Items Selected</b>
1 - Charges to Expired Awards	89	159,145	30
2 - Excess Salary	1,723	2,804,639	30
3 - High Risk Adjustments	488	554,558	30
4 - Admin Salaries	104	38,528	30
5 - All Other Transactions	7,272	8,358,124	60
<b>TOTALS</b>	<b>9,676</b>	<b>\$11,914,994</b>	<b>180</b>

**Method for Selecting Sample Units:** We arranged the transactions within each stratum in date order pursuant to the general ledger posting date as provided by GMU in its data. We then consecutively numbered the transactions within each stratum. After generating random numbers for each stratum using the U.S. Health and Human Services, Office of Inspector General, Office of Audit Services (HHS OIG/OAS) statistical software, we selected the corresponding frame items.

---

## Sample Results

---

**Estimation Methodology:** We used the HHS OIG/OAS RAT-STATS variable appraisal program for stratified samples to estimate the amount of unallowable salary and wage costs claimed by GMU against NSF awards for the audit period.

In addition, we provided the 21 sample transactions that were determined to be in error to GMU staff and asked them to provide us with the (1) Fringe Benefit and (2) Facilities & Administrative (F&A) costs associated with those transactions. We then estimated the Fringe Benefits and F&A costs associated with the original sample transactions.

### Results: Payroll Transactions (Salary and Wage Costs)

<b>Stratum</b>	<b>Frame Size</b>	<b>Value of Frame</b>	<b>Sample Size</b>	<b>Value of Sample</b>	<b>Number of Transactions in Error</b>	<b>Value of Transactions in Error</b>
1	89	\$159,145	30	\$65,265	2	\$ 1,121.82
2	1,723	2,804,639	30	49,680	7	10,959.67
3	488	554,558	30	25,748	4	5,538.90
4	104	38,528	30	9,684	0	0
5	7272	8,358,124	60	58,817	8	5,765.07

<b>Total</b>	<b>9,676</b>	<b>\$11,914,994</b>	<b>180</b>	<b>\$209,194</b>	<b>21</b>	<b>\$ 23,585.46</b>
--------------	--------------	---------------------	------------	------------------	-----------	---------------------

*Results: Fringe Benefits*

<b>Stratum</b>	<b>Frame Size</b>	<b>Sample Size</b>	<b>Number of Transactions in Error</b>	<b>Value of Transactions in Error</b>
1	89	30	2	\$ 287.18
2	1,723	30	6	2,012.99
3	488	30	4	1,243.82
4	104	30	0	0
5	7272	60	2	274.57
<b>Total</b>	<b>9,676</b>	<b>180</b>	<b>14</b>	<b>\$ 3,818.56</b>

*Results: F&A COSTS*

<b>Stratum</b>	<b>Frame Size</b>	<b>Sample Size</b>	<b>Number of Transactions in Error</b>	<b>Value of Transactions in Error</b>
1	89	30	2	\$ 635.46
2	1,723	30	7	5,409.72
3	488	30	4	3,086.14
4	104	30	0	0
5	7272	60	8	2,761.13
<b>Total</b>	<b>9,676</b>	<b>180</b>	<b>21</b>	<b>\$ 11,892.44</b>

Total Estimated Value<sup>8</sup> of Salary and Associated Costs for Transactions in Error

Category	Point Estimate	Adjusted Lower Limit <sup>9</sup>	Upper Limit
Salaries/Wages <sup>10</sup>	██████████	██████████	██████████
Fringe Benefits <sup>11</sup>	██████████	██████████	██████████
F&A Costs <sup>12</sup>	██████████	██████████	██████████
<b>Totals</b>	\$2,105,021.47	\$1,089,413.89	\$3,117,000.47

---

<sup>8</sup> We calculated the Estimates and Limits for a 90-Percent Confidence Interval.

<sup>9</sup> To be conservative, we used the “lower limit” amounts in our audit report, adjusted as noted in notes 9, 10, and 11.

<sup>10</sup> We did not use the results from strata 1 and 3 in calculating the estimated overpayments. Instead, we added the actual overpayments from stratum 1 (\$1,122) and stratum 3 (\$5,539) to the lower limit (\$702,403), which resulted in an adjusted lower limit of \$709,064.

<sup>11</sup> We did not use the results from strata 1, 3, and 5 in calculating the estimated overpayments. Instead, we added the actual overpayments from strata 1 (\$287), 3 (\$1,244) and 5 (\$275) to the lower limit (\$35,359), which resulted in an adjusted lower limit of \$37,165.

<sup>12</sup> We did not use the results from strata 1 and 3 in calculating the estimated overpayments. Instead, we added the actual overpayments from stratum 1 (\$635) and 3 (\$6,783) to the lower limit (\$339,464), which resulted in an adjusted lower limit of \$346,882.

---

## Appendix E: Additional Details on Information Technology

### General Controls

---

***GMU did not employ two-factor authentication to access Banner.***

Two-factor authentication, which is commonly found in electronic computer verification, is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as security code. In this context, the two factors involved are referred to as something you have and something you know. A common example of two-factor authentication is a bank card: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. A more advanced method is using a username and a token with a PIN that changes frequently.

***GMU did not adequately manage access controls for accounts in the Banner Oracle database and on Thuban.***

NIST defines “access control policies” (e.g., identity-based policies, role-based policies, attribute-based policies) and “access enforcement mechanisms” (e.g., access control lists, access control matrices, cryptography) as those controls employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

GMU did not adequately manage access controls for the accounts in the Banner Oracle database and on Thuban (the Unix server which houses the Oracle database). The auditors scanned the Banner Oracle database and found the following conditions:

- Three accounts with [REDACTED]
- 19 accounts with [REDACTED] Some of these are service accounts<sup>13</sup> with [REDACTED]
- 146 accounts [REDACTED]. 132 of these accounts [REDACTED].
- 701 accounts [REDACTED] [REDACTED] of the auditor’s scan, but [REDACTED]. [REDACTED].

On Thuban, the auditors examined the Unix accounts and found of the 184 reviewed, 26 appeared to not be in use. GMU staff reviewed the auditors’ results and concluded that nine accounts are eligible for removal.

---

<sup>13</sup> Service accounts do not refer to a person, and password assignments for service accounts do not go through the GMU password system. They are accounts that are created by the system staff or a software vendor and used by the computer system for processing.

<sup>14</sup> Representing the GMU 180-day password rotation cycle plus a 30-day buffer.

GMU Policy Number 1312, “Physical and Logical Access Security,” states that GMU will use “all reasonable IT security controls” to:

- Protect university information resources against unauthorized access and use
- Maintain the integrity of university data
- Ensure university data residing on any IT system is available when needed
- Comply with the appropriate Federal, state and other legislative, regulatory and industry requirements

The policy also requires prompt deactivation or disabling of accounts when necessary, including but not limited to accounts subject to the following circumstances:

- at the end of the individual’s employment or when continued access is no longer required;
- when employees are transferred, to ensure changes in access privileges are appropriate to the change in job function or location; or
- when employees are not working due to any sort of leave, disability or other authorized purpose, or when continued access is no longer required, for a period consistent with the employee’s personal usage needs and duration of absence.

The GMU Technology Systems Division website requires users to change their passwords every 180 days. The website also suggests that users do not use passwords that can be “easily guessed” or include the user’s username.

***GMU did not install security patches to the Oracle database in a timely manner.***

The Government Accountability Organization (GAO) has long recognized the importance of patch management<sup>15</sup>, which HHS-OIG defines as the process of identifying, reporting, and effectively remediating information system flaws in an operational system. Timely patching helps organizations maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain stability of the production environment. Organizations that cannot establish a mature information security control program that is based on a rigorous set of controls and processes within their information security environment might have a number of security vulnerabilities that, if exploited, could lead to unauthorized access of sensitive data. Minimizing this threat requires organizations to have properly configured systems, to use the latest software supported by the vendor, and to have the recommended efficiency and security patches installed.

---

<sup>15</sup> <http://www.gao.gov/assets/120/110330.html>

In addition to the late installation of the April and July 2013 patches, the auditors found that five other security patches were not installed in a timely manner, as noted below:

Patch Number	Month Issued	Month Installed	Elapsed Time
16056266	April 2013	August 2013	3 months
14727310	January 2013	August 2013	7 months
14275605	October 2012	August 2013	8 months
14727315	January 2013	April 2013	3 months
14275621	October 2012	April 2013	6 months

NIST Special Publication 800-40, Version 2.0, “Creating a Patch and Vulnerability Management Program,” states, “Timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is one of the most common issues identified by security and IT professionals.”

NIST Special Publication 800-53, Revision 3, “Recommended Security Controls for Federal Information Systems and Organizations,” provides guidance regarding patch management, and recommends that organizations (including any contractor to the organization) promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes).

***GMU did not update the Risk Assessment for Banner to reflect significant changes to the system.***

The introduction to NIST’s guidance on risk assessments summarizes the invaluable benefit of this control:

Organizations in the public and private sectors depend on information technology and information systems to successfully carry out their missions and business functions. Information systems can include very diverse entities ranging from office networks, financial and personnel systems, to very specialized systems.

Information systems are subject to serious threats that can have adverse effects on organizational operations and assets, individuals, or other organizations. By exploiting both known and unknown vulnerabilities, users can compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information systems can include purposeful attacks, environmental disruptions, human/machine errors, and structural failures. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

Risk assessment is one of the fundamental components of an organizational risk management process. Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), resulting from the operation and use of information systems. The purpose of risk assessments is to inform decision makers and support risk responses by identifying: (i) relevant threats to



organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk. Risk assessments can be conducted at all three tiers in the risk management hierarchy—including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level).

NIST Special Publication 800-30, “Guide for Conducting Risk Assessments,” provides guidance for updating risk assessments, noting that organizations should update existing risk assessments using the results from ongoing monitoring of risk factors. The guidance also states that if significant changes have occurred since the risk assessment was conducted, organizations can revisit the purpose, scope, assumptions, and constraints of the assessment to determine whether all tasks in the risk assessment process need to be repeated.