OPERATIONS COMMITTEE BULLETIN 12-09

TO: FWCJUA Operations Committee

FROM: Laura S. Torrence, Executive Director

DATE: August 22, 2012

RE: AUGUST 29, 2012 OPERATIONS COMMITTEE TELECONFERENCE MEETING AGENDA

Enclosed for your review is the agenda for the FWCJUA Operations Committee teleconference meeting scheduled for 10:00 a.m. (Eastern Time), August 29, 2012. Please contact me should you have any questions regarding the agenda for this meeting.

Enclosure

c: FWCJUA Board of Governors
   Tom Maida, General Counsel
   Jim Watford, Florida Office of Insurance Regulation
   FWCJUA Interested Parties (Please contact Kathy Coyne at 941-378-7408 to participate in this teleconference meeting.)
AGENDA FOR THE MEETING OF THE OPERATIONS COMMITTEE OF THE
FLORIDA WORKERS' COMPENSATION JOINT UNDERWRITING ASSOCIATION, INC.
TO BE HELD ON AUGUST 29, 2012 AT 10:00 A.M. VIA TELECONFERENCE

I. CALL TO ORDER & OPENING REMARKS Brett Stiegel
II. ANTI-TRUST PREAMBLE (Attachment A) Tom Maida
III. BANKING MATTERS (Attachment B) Dave Webber
IV. DISASTER RECOVERY MATTERS (Attachment C) Laura Torrence
V. TRAVELERS' SERVICE PROVIDER AUDIT RESULTS (Attachment D) Michael Cleary
VI. IT AUDIT (Attachment E) Laura Torrence
VII. PRELIMINARY 2013 BUSINESS PLAN & FORECAST (Attachment F) Laura Torrence
VIII. POLICY ADMINISTRATION/MANAGED CARE
SERVICE PROVIDER ENGAGEMENT (Attachment G) Laura Torrence
IX. REPORT ON OPERATIONS (Attachment H) Michael Cleary
X. GENERAL ANNOUNCEMENTS Brett Stiegel
XI. ADJOURNMENT & CLOSING REMARKS Brett Stiegel
ANTI-TRUST PREAMBLE

We are here to discuss and act on matters relating to the business of the Florida Workers' Compensation Joint Underwriting Association (FWCJUA) and not to discuss or pursue the business interests of our individual funds or companies.

We should proceed with caution and alertness towards the requirements and prohibitions of federal and state anti-trust laws.

We should not engage in discussions – either at this meeting or in private conversations – of our individual fund’s or companies’ plans or contemplated activities. We should concern ourselves only with the business of the Florida Workers’ Compensation Joint Underwriting Association as set forth in the agenda for this meeting.

Only FWCJUA market matters may be discussed at the meeting and each fund’s or company’s voluntary market plans cannot be discussed.
At the Investment Committee’s request, the Operations Committee shall consider the FWCJUA’s risk associated with having significant balances with any one commercial bank.

By way of background, the FWCJUA went through an RFP process overseen by the Operations Committee in late 2010 which resulted in JPMorgan Chase being selected to serve as the FWCJUA’s sole commercial bank. To date, the FWCJUA has never felt the need to consider multiple commercial banking relationships to manage the cash for day-to-day operations. Further, until 2011, the FWCJUA did not maintain savings accounts for investment purposes within its commercial bank and only kept between 3 to 6 months of cash flow needs at the bank to pay claims and operational expenses. However, in 4Q 2010 cash began to accumulate in savings accounts given the resignation of the investment manager. Given the short maturity duration of the FWCJUA’s investments, cash continued to accumulate in 2011 as the investment manager selected in April 2011 struggled to produce a suitable investment strategy for the FWCJUA’s consideration. The investment manager advised, although not usually preferred, that it was comfortable with the concentration risk at JP Morgan Chase in the current environment given alternative available quality investments were offering lower yields. Since Prime began executing the new investment strategy adopted July 16th and the 2004-2005 tier return of premium dividend checks were issued on July 31st, the cash balances have dissipated significantly from $39.3 million to $21.9 million and will continue to shrink while Prime completes its mission to fully invest available funds over the next two months.

Given the Investment Committee’s concern, staff has reviewed the organization’s anticipated operating cash flow needs. The FWCJUA’s arrangement with Travelers provides for a net monthly settlement of all premium payments collected, claims and producer fees paid by Travelers as well as its service fee. For the near term, this net cash flow is expected to remain neutral to slightly positive and therefore does not need to be considered from a cash flow funding perspective. The other major cash outflows to be considered would be general & administrative (G&A) expenses and reinsurace premiums. These are expected to total approximately $6.4 million annually. Given such, staff recommends that the FWCJUA retain a minimum of 6 months equivalent of this amount or $3.2 million at JP Morgan Chase.

With regard to the $3.2 million cash retention, staff recommends that approximately $1.8 million of this reside in the operating checking account wherein the FWCJUA receives a bank credit to offset most of its bank charges. As this is a non-interest bearing account, it is currently 100% insured by the FDIC; however, absent further action from Congress or the FDIC, balances above $250,000 will not be insured beyond December 31, 2012. Thus, the Committee’s consideration of sweep account alternatives for checking account balances in November may be warranted. Staff further recommends that approximately $1.4 million continue to be held in the saving accounts, currently paying 0.50% interest. The saving account balances would be consistent with the Investment Policy mandate that no more than 2% of the overall investable assets be held in any one BBB or better security. Thus, the acquisition of JPMorgan Chase commercial paper and bonds would be limited based upon the savings account balances.

With regard to risk mitigation beyond December 31, 2012, there are nightly sweep opportunities that can move the balances into alternative overnight investments such as Treasury or other security backed repurchase agreements or mutual funds and remote disbursement account strategies. These alternatives typically yield much less than the savings account in this investment environment. Staff will have these alternatives reviewed and priced for both the Operations Committee and Investment Committee meetings in November.

An exception to the cash retention policy suggested above would occur should the Board resolve to fund a return of premium policyholder dividend in the future as such outflows are normally more than anticipated above. However, risk may be mitigated with improved asset liability planning and the introduction of a sweep alternative for the dividend disbursement account. Further, it should be noted that the FWCJUA is currently holding Subplan D money in one of its savings accounts as it anticipates the return of the unused monies to the state at year end.

The Committee shall determine whether to establish retaining a minimum of $3.2 million to support cash outflow needs for G&A and reinsurance premiums, targeting $1.8 million as the average balance in the operations checking account with the remaining balance in savings accounts.
The Operations Committee shall confirm the Executive Director’s modifications to the Disaster Recovery & Emergency Preparedness Plan (DR&EP Plan) appendices listed below that were issued on August 17th.

1. Appendix A: Distribution List
2. Appendix C: Global Speed Dial Directory
   Global E-mail Directory
3. Appendix F: FWCJUA Master Vendor Contacts & Phone Numbers

Appendices A & C were updated to identify current employees on the Employee Contact List, Global Email and Speed Dial. Appendix F was updated to identify current vendors and contract dates. Appendix G was updated to identify current passwords and network configuration.

The Committee shall confirm the revisions to the DR&EP Plan.
The Committee shall receive a report on the FWCJUA performance audit of the policy administration and managed care service provider, Travelers.

Staff conducted a performance audit of Travelers on July 27-31, 2012. The performance audit resulted in a cumulative score of 99.4% and an overall “Commendable” rating for Travelers. This is a slight improvement from the last comprehensive performance audit staff conducted in 2011, which reflected a cumulative score of 97.2% and an overall “Commendable” rating. Following are the performance audit results for the five key performance areas tested.

<table>
<thead>
<tr>
<th>Key Performance Areas Tested</th>
<th>Compliance Percentage</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Underwriting &amp; Policy Issuance</td>
<td>100.0%</td>
<td>Commendable</td>
</tr>
<tr>
<td>Preliminary Audit</td>
<td>100.0%</td>
<td>Commendable</td>
</tr>
<tr>
<td>Loss Prevention</td>
<td>96.5%</td>
<td>Commendable</td>
</tr>
<tr>
<td>Premium Audit</td>
<td>100.0%</td>
<td>Commendable</td>
</tr>
<tr>
<td>Claims</td>
<td>100.0%</td>
<td>Commendable</td>
</tr>
<tr>
<td><strong>Cumulative Score</strong></td>
<td><strong>99.4%</strong></td>
<td><strong>Commendable</strong></td>
</tr>
</tbody>
</table>

The following rating key was utilized to score the five key performance areas tested.

<table>
<thead>
<tr>
<th>Compliance %</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>95 – 100</td>
<td>Commendable</td>
</tr>
<tr>
<td>87 – 94</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>80 – 86</td>
<td>Marginal</td>
</tr>
<tr>
<td>&lt; 80</td>
<td>Unsatisfactory</td>
</tr>
</tbody>
</table>

During the performance audit, staff again reviewed Travelers’ Anti-Fraud, Business Continuity Management (Disaster Recovery) and Document Retention Plans and found them to be comprehensive and adequate.

Overall, the Travelers’ dedicated units for the FWCJUA continue to be well run, and perform well in all aspects of policy administration. There continues to be a positive working relationship between the FWCJUA and the Travelers’ management team as well as the Travelers’ front line personnel.

**No Committee action is required on this agenda item.**
The Committee shall receive RSM McGladrey’s report on the results of the 2012 IT security audit and shall consider the on-going need for such audits.

In July, RSM McGladrey conducted its “internal” audit of the FWCJUA’s Disaster Recovery Plan related to IT systems. The audit tested both internal and external network security, including wireless and firewall security, for which the FWCJUA received an overall “Satisfactory” rating. Attached for the Committee’s review is RSM McGladrey’s report regarding the audit. All control concerns identified in the report have been addressed and are so noted in the report. **No Committee action is required on the report**; however, consideration should be given to the need for additional IT audits of this nature.

By way of background, in May 2008, the FWCJUA issued a Quote Solicitation for the purpose of engaging a reputable independent accounting or consulting firm with sufficient resources to assist the FWCJUA in conducting an “internal” audit of the FWCJUA’s disaster recovery plan related to IT systems, to include security, documentation, and support. The purpose of this “internal” audit was to ensure the security of IT systems as well as the reliability of the documentation for IT systems disaster recovery. The FWCJUA’s goal was to have reasonably secure, documented IT systems and procedures to timely recover and continue operations in the case of any type of emergency or disaster impacting systems, facilities, or IT personnel. RSM McGladrey, Inc. was ultimately engaged as the FWCJUA’s IT systems disaster recovery auditor. The three-year contract resulted in fees of just over $50K. The first year of the contract (2008) reviewed the security of IT systems as well as the reliability of the documentation for IT systems disaster recovery at a cost of approximately $35K, while the second and third year (2009 & 2010) reviews concentrated specifically on network security at a cost of approximately $7.5K per year. Further, the engagement was extended for two one-year extensions (2011 & 2012) concentrating specifically on network security at a cost of $7,500 per year.

RSM McGladrey’s initial review disclosed that the FWCJUA had assembled an extensive business continuity plan (BCP) that includes provisions for disaster recovery (DR) and business resumption. Further, the FWCJUA’s BCP documentation appeared to be relatively mature, it was clear that the organization was truly committed to business continuity planning. The initial evaluation identified a number of opportunities for FWCJUA to increase the usability of its BCP documentation and enhance the overall effectiveness of the organization’s disaster prevention and recovery planning initiative, all of which were assessed and implemented as deemed cost effective. All subsequent network security reviews resulted in overall “Satisfactory” ratings. Further, the FWCJUA was generally advised that its security was above other peers and very, very positive.

At this time, staff is suggesting that the 2013 Business Plan contemplate the creation of internal IT audit procedures for systems and security to be performed and documented at least twice yearly in lieu of outsourcing the IT audit. It is believed that internal auditing would be more current given a semi-annual review as well as more cost effective. Further, future outsourced IT audits may always be requisitioned as warranted, particularly when significant reconfigurations or overhauls to the infrastructure necessitate.

The Committee shall determine whether to incorporate into the 2013 Business Plan the creation of internal IT audit procedures for systems and security to be performed and documented at least twice yearly in lieu of outsourcing the IT audit.
Florida Workers’ Compensation Joint Underwriting Association, Inc.

Information Systems Security Review Services

August 16, 2012
August 16, 2012

Mr. Marc Babin
Florida Workers’ Compensation Joint Underwriting Association, Inc.
6003 Honore Avenue, Suite 204
Sarasota, Florida  34238

Dear Mr. Babin:

This report contains our findings and recommendations relating to the information systems (IS) security review services, which entailed performing the external and internal network security reviews, and wireless security reviews for Florida Workers’ Compensation Joint Underwriting Association, Inc. (FWCJUA). We have included our findings and recommendations as an attachment to this letter.

No assessment of controls or security can ever provide total assurance or 100 percent protection against possible control failures or security intrusions on your systems. The potential effectiveness of specific controls and security measures is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, information networks, applications and control environments are extremely dynamic in nature and our examination of your control and security methods and procedures are conducted and documented as of the following specific periods in time:

<table>
<thead>
<tr>
<th>Assessment Service</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Network Security Review</td>
<td>06/25/2012</td>
<td>06/29/2012</td>
</tr>
<tr>
<td>Internal Network Security Review</td>
<td>06/25/2012</td>
<td>06/27/2012</td>
</tr>
<tr>
<td>Wireless Network Security Review</td>
<td>06/25/2012</td>
<td>06/27/2012</td>
</tr>
<tr>
<td>Firewall Security Review</td>
<td>06/25/2012</td>
<td>06/27/2012</td>
</tr>
</tbody>
</table>

As a result, the projection of any conclusions, based on our examination, to future periods is subject to the risk that (1) changes are made to the systems or controls; (2) changes are made in processing requirements; (3) changes are required because of the passage of time; or (4) new security exploits are discovered that may alter the validity of such conclusions. Therefore, McGladrey LLP takes no responsibility for any lack of specific controls, control failures, breach of security, or other errors or fraud related to any part of your business environment other than those controls and security measures specifically examined and for any period of time other than the period specifically covered by our assessment conducted. Any subsequent control or security issues that may arise within those areas examined or any control or security issues that are present at the time of this examination, but that are outside the scope of the examination, are solely the responsibility of FWCJUA.

This report is intended solely for use by the management of FWCJUA, its internal and external auditors, and its regulatory examiners.

We appreciate the courtesies and cooperation extended to us during this project and appreciate the opportunity to be of service to FWCJUA. Please contact Loras Even at 319.274.8541 or Alexandra Lorie at 305.742.7117 if you have any questions regarding this report.

Sincerely,

[Signature]
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. <strong>PROJECT BACKGROUND</strong> ..................................................................</td>
<td>1</td>
</tr>
<tr>
<td>A. BACKGROUND</td>
<td>1</td>
</tr>
<tr>
<td>B. OBJECTIVES OF THIS PROJECT</td>
<td>1</td>
</tr>
<tr>
<td>C. SCOPE</td>
<td>1</td>
</tr>
<tr>
<td>D. APPROACH</td>
<td>2</td>
</tr>
<tr>
<td>II. <strong>EXECUTIVE SUMMARY</strong> ..................................................................</td>
<td>6</td>
</tr>
<tr>
<td>A. EXTERNAL NETWORK SECURITY REVIEW</td>
<td>6</td>
</tr>
<tr>
<td>B. INTERNAL NETWORK SECURITY REVIEW</td>
<td>7</td>
</tr>
<tr>
<td>C. WIRELESS NETWORK SECURITY REVIEW</td>
<td>7</td>
</tr>
<tr>
<td>D. FIREWALL SECURITY REVIEW</td>
<td>8</td>
</tr>
<tr>
<td>III. <strong>CONTROL CONCERNS</strong></td>
<td>10</td>
</tr>
<tr>
<td>IV. <strong>EXTERNAL NETWORK SECURITY FINDINGS AND RECOMMENDATIONS</strong> ..........</td>
<td>12</td>
</tr>
<tr>
<td>A. WEAK ENCRYPTION PROTOCOL—SECURE SOCKET LAYER (SSL) v2</td>
<td>12</td>
</tr>
<tr>
<td>B. SELF-SIGNED SSL CERTIFICATE</td>
<td>12</td>
</tr>
<tr>
<td>C. EXPIRED SSL CERTIFICATE</td>
<td>13</td>
</tr>
<tr>
<td>D. WEAK ENCRYPTION ALGORITHM</td>
<td>14</td>
</tr>
<tr>
<td>E. CREDENTIAL LEAKAGE—AUTOCOMPLETE</td>
<td>14</td>
</tr>
<tr>
<td>V. <strong>INTERNAL NETWORK SECURITY FINDINGS AND RECOMMENDATIONS</strong> ..........</td>
<td>16</td>
</tr>
<tr>
<td>A. MISSING CRITICAL PATCH—DNS SERVERS</td>
<td>16</td>
</tr>
<tr>
<td>B. MISSING CRITICAL PATCH—TERMINAL SERVICES</td>
<td>16</td>
</tr>
<tr>
<td>C. MISSING PATCHES—VMWARE ESX/ESXI</td>
<td>17</td>
</tr>
<tr>
<td>D. PASSWORD POLICY BYPASS—NEC PHONE SYSTEM</td>
<td>18</td>
</tr>
<tr>
<td>E. MICROSOFT PATCHES</td>
<td>19</td>
</tr>
<tr>
<td>F. ACCESS WITH DEFAULT CREDENTIALS—NEC UNIVERGE UM8000</td>
<td>23</td>
</tr>
<tr>
<td>G. SERVER MESSAGE BLOCK (SMB) NULL SESSION AUTHENTICATION</td>
<td>23</td>
</tr>
<tr>
<td>VI. <strong>WIRELESS NETWORK SECURITY FINDINGS AND RECOMMENDITIONS</strong> ..........</td>
<td>25</td>
</tr>
<tr>
<td>A. WIRELESS NETWORK ENCRYPTION</td>
<td>25</td>
</tr>
<tr>
<td>B. ENCRYPTION KEY</td>
<td>25</td>
</tr>
<tr>
<td>C. GEOGRAPHIC COVERAGE</td>
<td>25</td>
</tr>
<tr>
<td>D. ENCRYPTION LEVEL</td>
<td>27</td>
</tr>
<tr>
<td>E. ACCESS POINT HARDWARE IMPLEMENTED</td>
<td>27</td>
</tr>
<tr>
<td>F. ACCESS POINT CONFIGURATION</td>
<td>27</td>
</tr>
<tr>
<td>VII. <strong>FIREWALL SECURITY OBSERVATIONS</strong></td>
<td>28</td>
</tr>
<tr>
<td>A. EXTENSIVE OPEN PORTS—EXTERNAL INTERFACE</td>
<td>28</td>
</tr>
</tbody>
</table>

© 2012 McGladrey LLP. All Rights Reserved.
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIII. Exhibits</td>
<td>29</td>
</tr>
<tr>
<td>A. Tools Utilized</td>
<td>29</td>
</tr>
<tr>
<td>B. Footprinting Information</td>
<td>30</td>
</tr>
<tr>
<td>C. Enumeration Information</td>
<td>30</td>
</tr>
<tr>
<td>D. Vulnerability Report Key</td>
<td>30</td>
</tr>
<tr>
<td>E. External Vulnerability Reports</td>
<td>31</td>
</tr>
<tr>
<td>F. Internal Vulnerability Reports</td>
<td>31</td>
</tr>
</tbody>
</table>
I. PROJECT BACKGROUND

A. BACKGROUND

Security of technology assets has always been a high priority. However, with the advent of electronic commerce, the security of technology has become even more important as companies and their business partners have connected their networks to the Internet.

B. OBJECTIVES OF THIS PROJECT

The primary objectives of the project were to perform:

- A network security review of your publicly available, Internet computing systems
- A network security review of your internal systems
- A wireless network security review
- A firewall security review

Our analysis used a multifaceted approach, including the use of automated and manual tools to determine the ability of unauthorized persons to access Florida Workers’ Compensation Joint Underwriting Association, Inc.’s (FWCJUA’s) network infrastructure and hosts, including your internal and external network, wireless networks and local computing assets.

The management of FWCJUA is responsible for establishing and maintaining controls. The objective of the overall information security review is to provide management with reasonable, but not absolute, assurance that assets are safeguarded against loss, unauthorized use or disposition. In establishing internal and external controls related to information systems (IS), estimates and judgments by management are required to assess the expected benefits and related costs of controls.

Because of inherent limitations in any controls, errors or fraud may occur and not be detected. Also, projection of any evaluation of the controls to future periods is subject to the risk that the controls may become inadequate because of changes in the control environment, or that the degree of compliance with the controls may deteriorate.

C. SCOPE

The scope of our review consisted of four areas:

- External network security review

  The scope of the review focused on the security controls of the external network servers and their associated applications and operating systems. Accordingly, we conducted our testing to determine the effectiveness of the logical security controls surrounding these systems.

- Internal network security review

  The scope of the network review included identification of hosts on the internal network physically located at various FWCJUA locations. The McGladrey LLP network security methodology was used to enumerate hosts and services on the local network, identify software vulnerabilities and misconfigurations, exploit identified vulnerabilities and escalate local access privileges to the highest levels available.
• Wireless network security review
  For the wireless network security review we reviewed the security posture of the wireless networks for the Sarasota headquarters.

• Firewall security review
  We reviewed the firewall configurations for the firewalls at the Sarasota headquarters and associated disaster recovery site.

D. APPROACH

To accomplish our objectives, we organized this project into the following activities:

Phase I: External Network Security Review

Activities performed included:

• Footprinting
  The footprinting process was used to determine the amount of information available through public sources concerning your organization. Our footprinting process included, but was not limited to, the following activities:
  - Mapping of domain names used
  - Mapping of domains linked to your domain names used
  - American Registry of Internet Number (ARIN) searches
  - Domain Name Service (DNS) lookups
  - Traceroutes of public systems

• Basic vulnerability testing
  Basic vulnerability testing involved using various commercial and open-source tools to conduct further security testing. Our basic vulnerability testing included, but was not limited to:
  - Ping scans of public Internet Protocol (IP) address blocks
  - Port scans of public systems
  - Basic vulnerability testing using commercial and open-source tools to determine how much information could be harvested from your public computing assets

• Advanced vulnerability testing
  Advanced vulnerability testing involved running the vulnerability testing tools more aggressively as appropriate, and sorting and verifying the results. The results were verified through manual efforts to reduce the likelihood of false positive vulnerabilities being reported. This provided you with specific and appropriate remediation recommendations based on real vulnerabilities in consideration of the device type being tested.
Examples of some common devices tested, verified and reported on include:

- Network infrastructure, such as routers and switches
- Security infrastructure, such as firewalls and intrusion detection/prevention systems
- Web servers
- Electronic mail servers
- Other servers, such as those for file transfers, remote device control or other non-Web services
- VPN servers
- Other public devices, as required

During our vulnerability testing, we conducted tests against the aforementioned devices. These tests included denial of service, port redirects, certain advanced application tests, such as cross-site scripting and buffer overflows and other, more severe or extreme vulnerability tests. While this testing involved some application vulnerability-like tests, this testing is not a replacement for application vulnerability testing and cannot be used as proof of an application vulnerability test.

**Phase II: Internal Network Security Review**

The objective of the internal network security review is to identify and demonstrate that exploitable internal network vulnerabilities exist, not to demonstrate that a network is free of all vulnerabilities.

Because we were behind your organization’s more rigorous security measures, we did not conduct testing that was as intrusive as external testing. Our testing was limited to basic tests designed for ensuring adequate security measures for an internal network.

Activities performed included, but were not limited to:

- **Internal network discovery**
  - Inventory scans of identified samples
  - Operating system identification and classification
  - Operating system-level scans (patches)
  - Implementation standards review (base image use, etc.)

- **Server-specific testing**
  - System hardening verification
    - Default services removed
    - Default shares removed or secured
- Simple Network Management Protocol (SNMP) and other enumeration tools hardened

- Scanning for remote control software, such as pcAnywhere, Carbon Copy, SubSeven, etc.

- User authentication
  - Default users changed or removed as appropriate
  - User authentication parameters
  - Inactive account review for domain controllers as appropriate

- Vulnerability scanning
  - Automated scans using Nessus and other automated tools
  - Manual testing using various open-source and customized tools

- Workstation-specific testing
  - System hardening verification
    - Default services removed
    - Default shares removed or secured
    - SNMP and other enumeration tools hardened
    - Scanning for remote control software, such as pcAnywhere, Carbon Copy, SubSeven, etc.

- Vulnerability scanning
  - Automated scans using Nessus and other automated tools
  - Manual testing using various open-source and customized tools

- Network device testing
  - Configuration review
    - Core device configuration review from a security standpoint
    - Management system review (user access, device database security, alarm profiles)

  - Vulnerability scanning
    - Automated scans using various commercial and open-source tools
    - Manual testing using various open-source and customized tools
- Network administration and defense measures
  - Patching systems and methods
  - Virus protection measures and enforcement
  - System hardening techniques pre-rollout and post-rollout
  - Device change management controls

**Phase III: Wireless Network Security Review**

The objective of the wireless network security review was to identify and demonstrate that exploitable wireless network vulnerabilities exist, not to demonstrate that these networks are free of all vulnerabilities.

Because FWCJUA had implemented 802.11 wireless networking, we conducted wireless network security tests to determine the effectiveness of your wireless security measures based on whether your wireless networks were public and/or private. Our tests included but were not limited to:

- Assessed all facilities that had been identified by FWCJUA’s technology personnel that contained wireless networks using various wireless networking identification tools or scanners
- Reviewed all access point configurations
- Assessed the key strength of the wireless encryption keys (based on the results of the aforementioned steps)

**Phase IV: Firewall Security Review**

The firewall security review included checking for common misconfigurations and the state of the established rules. These tests included, but were not limited to, passwords, missing patches, disabled, duplicate and or unused firewall rules, dangerous protocols and administration settings.

**Reporting**

We kept you informed of our progress throughout the engagement through periodic formal and informal status reports and meetings as appropriate. Upon completion of the review, we prepared this written report of our findings and recommendations.
II. EXECUTIVE SUMMARY

A. EXTERNAL NETWORK SECURITY REVIEW

Network security is a dynamic field with new exploits and revisions and updates to security standards occurring on a regular basis. In the 2011 Verizon Business Services Data Breach Investigations Report, published in September 2011, 92 percent of data breaches were the result of external agents. However, 96 percent of all data breaches could have been avoided had basic internal controls been implemented and functioning. Organizations have been taking more precautions such as decreasing the intervals between system audits, third-party security services, software, hardening techniques on system configurations, etc. All of the various security surveys McGladrey has reviewed indicate that the financial burden of cyber crimes continues to be detrimental to all industries.

Our external network security review was designed to answer the following questions for FWCJUA:

- **Was McGladrey able to compromise FWCJUA’s external network security?**
  
  **No.** During the conduct of our review, we were not able to compromise FWCJUA’s external network security. We were also unable to obtain any customer information or gain sufficient access to any of FWCJUA’s servers to gain control of those servers.

- **Did McGladrey identify any issues that FWCJUA should be aware?**
  
  **Yes.** Our review did identify some security issues related to FWCJUA’s external network. These issues are documented in detail in Section IV. External Network Security Findings and Recommendations.

- **What is McGladrey’s assessment of FWCJUA’s external network security?**

  Based on a review of the results of our activities, we believe overall, your external network security is **satisfactory** as of the date of our testing.

  A **satisfactory** designation indicates that while there may be security improvements identified, FWCJUA appears to have taken appropriate action to ensure the security of FWCJUA’s external network. However, a satisfactory designation should not be construed as absolute assurance that FWCJUA’s external network is completely protected from attacks and/or intrusions.

  A **needs improvement** designation indicates that, while FWCJUA has implemented some security measures, the security improvements identified are significant or pervasive enough that FWCJUA’s external network is at a higher-than-acceptable risk of a successful attack or intrusion.

  An **unsatisfactory** designation indicates that, based on the issues identified, FWCJUA does not appear to have taken appropriate action to ensure the security of FWCJUA’s external network.
B. INTERNAL NETWORK SECURITY REVIEW

In the 2011 Verizon Business Services Data Breach Investigations Report, published in September 2011, 17 percent of data breaches were the result of insider actions. However, 96 percent of all data breaches could have been avoided had basic internal controls been implemented and functioning. Organizations have been taking more precautions such as decreasing the intervals between system audits, third-party security services, software, hardening techniques on system configurations, etc. All of the various security surveys McGladrey has reviewed indicate that the financial burden of cyber crimes continues to be detrimental to all industries.

Our internal network security review was designed to answer the following questions for FWCJUA:

- **Could McGladrey compromise FWCJUA’s internal network?**
  
  No. During the conduct of our review, we were not able to identify vulnerabilities that would allow us to compromise FWCJUA’s internal network security. We were also unable to obtain customer information or any other relevant company information.

- **Did McGladrey identify any issues that FWCJUA should be aware?**
  
  Yes. Our review did identify some security issues that could allow unauthorized persons to cause service issues or potential outages related to FWCJUA’s internal network. These issues are documented in detail in Section V. Internal Network Security Findings and Recommendations of this report and are summarized here:

- **What is McGladrey’s assessment of FWCJUA’s internal network security?**

  Based on a review of the results of our activities, we believe overall, your internal network security is **satisfactory** as of the date of our testing.

  A **satisfactory** designation indicates that while there may be security improvements identified, FWCJUA appears to have taken appropriate action to ensure the security of FWCJUA’s internal network. However, a satisfactory designation should not be construed as absolute assurance that FWCJUA’s internal network is completely protected from attacks and/or intrusions.

  A **needs improvement** designation indicates that, while FWCJUA has implemented some security measures, the security improvements identified are significant or pervasive enough that FWCJUA’s internal network is at a higher-than-acceptable risk of a successful attack or intrusion.

  An **unsatisfactory** designation indicates that, based on the issues identified, FWCJUA does not appear to have taken appropriate action to ensure the security of FWCJUA’s internal network.

C. WIRELESS NETWORK SECURITY REVIEW

The use of wireless networks is attractive to many organizations in order to allow flexibility of movement for computer resources and to minimize investment in a fixed infrastructure. FWCJUA has implemented wireless networks for use by employees (Fwcjua) and guests (FwcjuaGuest).
Our wireless network security review was designed to answer the following questions for FWCJUA:

- **Was McGladrey able to compromise FWCJUA’s wireless networks?**
  
  No. During the conduct of our review, we were not able to compromise FWCJUA’s wireless network at your Sarasota data center. We were also unable to collect a substantial amount of data packets from FWCJUA’s wireless access points and were unable to collect the correct type of data packets in enough quantity to allow the cracking of the encryption method used by your wireless network.

- **Did McGladrey identify any issues that FWCJUA should be aware?**
  
  No. Our review did not identify any significant security issues that could cause operational or security issues with your wireless network.

- **What is McGladrey’s assessment of FWCJUA’s wireless network security?**
  
  Based on a review of the results of our activities, we believe overall, your wireless network security is **satisfactory** as of the date of our testing.

  A **satisfactory** designation indicates that while there may be security improvements identified, FWCJUA appears to have taken appropriate action to ensure the security of FWCJUA’s wireless network. However, a satisfactory designation should not be construed as absolute assurance that FWCJUA’s wireless network is completely protected from attacks and/or intrusions.

  A **needs improvement** designation indicates that, while FWCJUA has implemented some security measures, the security improvements identified are significant or pervasive enough that FWCJUA’s wireless network is at a higher-than-acceptable risk of a successful attack or intrusion.

  An **unsatisfactory** designation indicates that, based on the issues identified, FWCJUA does not appear to have taken appropriate action to ensure the security of FWCJUA’s wireless network.

### D. Firewall Security Review

Our firewall security review was designed to answer the following questions for FWCJUA:

- **Did McGladrey identify any issues that FWCJUA should be aware?**
  
  Yes. Our review did identify some security issues that could cause operational or security issues with your firewall(s). These issues are documented in detail in Section VII. Firewall Security Findings and Recommendations:

- **What is McGladrey’s assessment of FWCJUA’s firewall network security?**
  
  Based on a review of the results of our activities, we believe overall, your wireless network security is **satisfactory** as of the date of our testing.

  A **satisfactory** designation indicates that while there may be security improvements identified, FWCJUA appears to have taken appropriate action to ensure the security of FWCJUA’s wireless network. However, a satisfactory designation should not be construed as absolute assurance that FWCJUA’s wireless network is completely protected from attacks and/or intrusions.
A **needs improvement** designation indicates that, while FWCJUA has implemented some security measures, the security improvements identified are significant or pervasive enough that FWCJUA’s wireless network is at a higher-than-acceptable risk of a successful attack or intrusion.

An **unsatisfactory** designation indicates that, based on the issues identified, FWCJUA does not appear to have taken appropriate action to ensure the security of FWCJUA’s wireless network.

No assessment of controls or security can ever provide total assurance or 100 percent protection against possible control failures or security intrusions on your systems. The potential effectiveness of specific controls and security measures is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, information networks, applications and control environments are extremely dynamic in nature and our examination of your control and security methods and procedures are conducted and documented as of the following specific periods in time:

<table>
<thead>
<tr>
<th>Assessment Service</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Network Security Review</td>
<td>06/25/2012</td>
<td>06/29/2012</td>
</tr>
<tr>
<td>Internal Network Security Review</td>
<td>06/25/2012</td>
<td>06/27/2012</td>
</tr>
<tr>
<td>Wireless Network Security Review</td>
<td>06/25/2012</td>
<td>06/27/2012</td>
</tr>
<tr>
<td>Firewall Security Review</td>
<td>06/25/2012</td>
<td>06/27/2012</td>
</tr>
</tbody>
</table>

As a result, the projection of any conclusions, based on our examination, to future periods is subject to the risk that (1) changes are made to the systems or controls; (2) changes are made in processing requirements; (3) changes are required because of the passage of time; or (4) new security exploits are discovered that may alter the validity of such conclusions. Therefore, McGladrey LLP takes no responsibility for any lack of specific controls, control failures, breach of security, or other errors or fraud related to any part of your business environment other than those controls and security measures specifically examined and for any period of time other than the period specifically covered by our assessment conducted. Any subsequent control or security issues that may arise within those areas examined or any control or security issues that are present at the time of this examination, but that are outside the scope of the examination, are solely the responsibility of FWCJUA.
III. CONTROL CONCERNS

A summary of our control findings is described below. These items are described in detail in Sections IV, V, VI and VII of this report. The attached chart outlines all of the control concerns identified during this engagement, including:

- Control Concern Description is a brief description of the control concern.

- Relative Risk is a subjective evaluation of the severity of the concern and the potential impact on the operations. Items rated “High” are of immediate concern and could cause significant operational issues if not addressed soon. Items rated “Medium” may also cause operational issues and do not require immediate attention but should be addressed as soon as possible. Items rated “Low” could escalate into operational issues but can be addressed through the normal course of conducting business. It should be noted that relative risk is not indicative of a security risk unless explicitly stated in the detailed finding and recommendation.

- Resolution Level of Difficulty is a subjective evaluation of the estimated level of difficulty to resolve the concern based on our experience and potential cost. Items rated “High” are considered to be difficult to resolve and/or will require a significant amount of planning and management involvement/oversight in order to obtain resolution. Items rated “Medium” are not as difficult to resolve and/or they do not require a significant amount of planning but may be time-consuming to resolve. Items rated “Low” are items that are not complex and/or do not require significant amounts of planning and time to resolve.

FWCJUA’s management should consider each control concern and develop a detailed action plan to address the issues identified in this report. The action plan should include:

- Action description

- Responsible party(ies)

- Target start date

- Target completion date

- Resource requirements

Management of FWCJUA should be directly involved in the implementation of this action plan to ensure that all issues are adequately resolved.
### Summary of Control Concerns

<table>
<thead>
<tr>
<th>Control Concern Description</th>
<th>Page</th>
<th>Relative Risk</th>
<th>Resolution Level of Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV. External Network Security Findings and Recommendations</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Weak Encryption Protocol—Secure Socket Layer (SSL) v2</td>
<td>12</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>B. Self-Signed SSL Certificate</td>
<td>12</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>C. Expired SSL Certificate</td>
<td>13</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>D. Weak Encryption Algorithm</td>
<td>14</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>E. Credential Leakage—Autocomplete</td>
<td>14</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>V. Internal Network Security Findings and Recommendations</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Missing Critical Patch—DNS Servers</td>
<td>16</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>B. Missing Critical Patch—Terminal Services</td>
<td>16</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>C. Missing Patches—VMWare ESX/ESXi</td>
<td>17</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>D. Password Policy Bypass—NEC Phone System</td>
<td>18</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>E. Microsoft Patches</td>
<td>19</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>F. Access With Default Credentials—NEC UniVerge UM8000</td>
<td>23</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>G. Server Message Block (SMB) Null Session Authentication</td>
<td>23</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>VI. Wireless Network Security Findings and Recommendations</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Wireless Network Encryption</td>
<td>25</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>B. Encryption Key</td>
<td>25</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>C. Geographic Coverage</td>
<td>25</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>D. Encryption Level</td>
<td>27</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>E. Access Point Hardware Implemented</td>
<td>27</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>F. Access Point Configuration</td>
<td>27</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>VII. Firewall Security Observations</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Extensive Open Ports—External Interface</td>
<td>28</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>

NA = Not Applicable
IV. EXTERNAL NETWORK SECURITY FINDINGS AND RECOMMENDATIONS

A. WEAK ENCRYPTION PROTOCOL—SECURE SOCKET LAYER (SSL) v2

Relative Risk: Medium
Resolution Level of Difficulty: Low

Finding:

The SSLv2 protocol is susceptible to vulnerabilities that would allow communications to be compromised. Attackers take advantage of weaknesses in the protocol to force low-grade encryption to be used to facilitate decryption attacks or to compromise message integrity. For information pertaining to the SSLv2 vulnerabilities, see http://www.schneier.com/paper-ssl.pdf.

Affected IP Addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>443 Transport Control Protocol (TCP)/Hypertext</td>
</tr>
<tr>
<td></td>
<td>Transport Protocol Secure (HTTPS)</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>443 TCP/HTTLS</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>443 TCP/HTTLS</td>
</tr>
</tbody>
</table>

Recommendation:

We recommend the use of the SSLv3 or Transport Layer Security (TLS) v1 encryption protocols, and we recommend disabling SSLv2. For more information regarding recommended encryption standards, see http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf. For information regarding the configuration of SSL on Internet Information Server (IIS), see http://support.microsoft.com/kb/187498/.

Management Response:

Both servers have been modified to force higher encryption.

Responsible Party: Marc Babin, IS Manager

Due Date: Completed

B. SELF-SIGNED SSL CERTIFICATE

Relative Risk: Low
Resolution Level of Difficulty: Low

Finding:

The encrypted service is using a self-signed SSL certificate. When SSL certificates are not signed by a third-party certificate authority, users cannot substantiate the authenticity of a service or any encryption keys exchanged. A malicious individual could create their own self-signed certificate to impersonate the legitimate service as part of a man-in-the-middle attack.
Affected IP Address:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>25 TCP/Simple Mail Transfer Protocol (SMTP) and 995 TCP/Post Office Protocol (POP) 3S</td>
</tr>
</tbody>
</table>

Recommendation:

We recommend obtaining an SSL certificate signed by a third-party certificate authority to establish the authenticity of the service and mitigate risks associated with man-in-the-middle attacks.

Management Response:

Email server is currently using the self-signed certificate as the current wildcard certificate does not function with POP3 services on Exchange 2010. We will replace the wildcard certificate at the next expiration. We will also evaluate the need for POP3.

Responsible Party: Marc Babin, IS Manager

Due Date: Completed

C. EXPIRED SSL CERTIFICATE

Relative Risk: Low
Resolution Level of Difficulty: Low

Finding:

The encrypted service is using an expired SSL certificate. SSL certificates are used to establish the authenticity of a service and need to be periodically replaced to ensure that the information on the certificate is accurate. If a service is using an expired SSL certificate, a user cannot substantiate the authenticity of the service or any authentication keys exchanged.

Affected IP Address:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>443 TCP/HTTPS</td>
</tr>
</tbody>
</table>

Recommendation:

We recommend obtaining a new third-party SSL certificate to replace the expired certificate.

Management Response:

Old certificate was still on test server and has been updated to the current certificate.

Responsible Party: Marc Babin, IS Manager

Due Date: Completed
D. **WEAK ENCRYPTION ALGORITHM**

Relative Risk: Low  
Resolution Level of Difficulty: Low

**Finding:**

The Secure Shell (SSH) service is accepting connections using weak encryption algorithms susceptible to a higher risk of being compromised. Minimum encryption standards have been raised because cryptanalysis techniques have improved and faster hardware implementations have decreased the computation time necessary to decrypt communications. The SSH-based RC4 algorithms are no longer recommended for use, [http://tools.ietf.org/html/rfc4345](http://tools.ietf.org/html/rfc4345). Malicious individuals can use network monitoring tools to capture communications protected with weak encryption and potentially decrypt the communications with brute-force techniques.

**Affected IP Address:**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>22 TCP/SSH and 830 TCP/SSH</td>
</tr>
</tbody>
</table>

**Recommendation:**

We recommend reconfiguring the SSH service to disable the RC4 encryption.

**Management Response:**

The device in question is the gateway on our hosting provider’s network. We will notify them of the findings.

**Responsible Party:** Marc Babin, IS Manager  
**Due Date:** Completed

E. **CREDENTIAL LEAKAGE—AUTOCOMPLETENESS**

Relative Risk: Low  
Resolution Level of Difficulty: Low

**Finding:**

The password input parameter and Hypertext Markup Language (HTML) FORM tag on the login page does not have “autocomplete” set to “off.” Browsers may be able to cache credentials that could be used by a malicious individual to access the service.

**Affected IP Addresses:**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port/Service</th>
<th>Uniform Resource Locators</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>443 TCP/HTTPS</td>
<td>/login/Login.aspx</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>443 TCP/HTTPS</td>
<td>/login.asp</td>
</tr>
</tbody>
</table>
Recommendation:

We recommend changing the HTML code setting the “autocomplete” element to “off” within the password input parameter or the HTML FORM tag to mitigate the risk of credential leakage.

Management Response:

This issue will be resolved as we are implementing a new single sign-on process for the websites.

Responsible Party: Marc Babin, IS Manager

Due Date: Completed
V. INTERNAL NETWORK SECURITY FINDINGS AND RECOMMENDATIONS

Security vulnerabilities, even on systems that are not exposed to the Internet, weaken the overall security posture of the organization and provide an easy target for an attacker in the event that the perimeter security of an organization is breached. Maintaining a strong internal network security posture in addition to perimeter security greatly reduces the possibility of an attacker compromising critical internal network systems, such as the core banking system.

A. MISSING CRITICAL PATCH—DNS SERVERS

Relative Risk: High  
Resolution Level of Difficulty: Low

Finding:

The DNS servers at addresses XXX.XXX.XXX.XXX (vm-dc01.fwcjua.com) and XXX.XXX.XXX.XXX (helios.fwcjua.com) are missing Microsoft patch MS11-058. This patch addresses critical security vulnerabilities in the DNS service.

Recommendation:

We recommend that management apply this critical patch to the affected systems. See http://technet.microsoft.com/en-us/security/bulletin/ms11-058 for instructions on obtaining and applying this update.

Status: This finding was remediated while we were on-site.

Management Response:

The patches have been installed. Our current maintenance plan for patches is on a monthly basis. Some of the general servers have been configured for automatic updates weekly.

Responsible Party: Marc Babin, IS Manager

Due Date: Completed

B. MISSING CRITICAL PATCH—TERMINAL SERVICES

Relative Risk: High  
Resolution Level of Difficulty: Low

Finding:

The affected terminal servers are missing Microsoft patch MS12-020. This patch addresses a critical security vulnerability in the Remote Desktop Protocol (RDP) service.

Affected IP Addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name</th>
<th>Port/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>docmgmt.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
</tbody>
</table>
### C. MISSING PATCHES—VMWARE ESX/ESXi

**Relative Risk:** High  
**Resolution Level of Difficulty:** Medium

**Finding:**  
The VMWare hosts at addresses XXX.XXX.XXX.XXX, XXX.XXX.XXX.XXX,  
XXX.XXX.XXX.XXX and XXX.XXX.XXX.XXX are missing critical patches that address

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name</th>
<th>Port/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>ts3.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>vm-jua06.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>phone1.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>phone2.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>rdg1.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>ts1.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>vm-oracle01.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>triton.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>ftp02.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>vm-web04.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>vm-web03.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>vm-web02.fwcjua.com</td>
<td>TCP 3389/RDP</td>
</tr>
</tbody>
</table>

**Recommendation:**  
We recommend that management apply this critical patch to the affected systems. See [http://technet.microsoft.com/en-us/security/bulletin/ms12-020](http://technet.microsoft.com/en-us/security/bulletin/ms12-020) for instructions on obtaining and applying this update.

**Status:** This finding was remediated while we were on-site.

**Management Response:**  
The patches have been installed. Our current maintenance plan for patches is on a monthly basis. Some of the general servers have been configured for automatic updates weekly.

**Responsible Party:** Marc Babin, IS Manager  
**Due Date:** Completed
multiple security vulnerabilities. For more information, see http://lists.vmware.com/pipermail/security-announce/2012/000175.html.

**Recommendation:**

We recommend that management work with the vendor to obtain and apply these critical updates.

**Management Response:**

The patches have been installed. Our current maintenance plan for patches is on a monthly basis.

**Responsible Party:** Marc Babin, IS Manager

**Due Date:** Completed

D. **PASSWORD POLICY BYPASS—NEC PHONE SYSTEM**

**Relative Risk:** High

**Resolution Level of Difficulty:** Medium

**Finding:**

The server at address XXX.XXX.XXX.XXX is running HylaFAX, a fax/pager server application for Linux/UNIX.

We were able to access this system using default credentials (login $nec with no password):
The version of HylaFAX installed on the server does not check passwords when authenticating users via hfaxd, its fax server on TCP Port 4559. An attacker can exploit this issue to bypass authentication using a valid username and gain access to the system. See also [http://www.hylafax.org/content/HylaFAX_4.2.4_release](http://www.hylafax.org/content/HylaFAX_4.2.4_release) for more information.

**Recommendation:**

We recommend that management work with the vendor to rebuild HylaFAX with Pluggable-Authentication Modules (PAM) support or upgrade to HylaFAX Version 4.2.4 or later and change this password to something other than the default.

**Management Response:**

This service on the phone system is not in use. We will contact the vendor to see if they can implement any changes or change passwords.

**Responsible Party:** Marc Babin, IS Manager

**Due Date:** Completed

---

**E. MICROSOFT PATCHES**

**Relative Risk:** Medium  
**Resolution Level of Difficulty:** Medium

**Finding:**

Many of the scanned systems are missing important Microsoft Windows patches. Below is a list of the system addresses and the missing patches:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Microsoft Patch Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-020,MS12-002,MS11-019,MS11-046,MS10-061,MS11-006,MS11-052,MS11-050,MS11-090,MS11-030,MS11-099,MS11-043,MS12-008,MS12-006,MS11-081,MS12-005,MS11-042,MS11-014,MS11-071,MS12-024,MS11-069,MS12-001,MS11-066,MS11-078,MS10-074,MS11-011,MS11-027,MS11-057,MS10-098,MS11-032,MS11-031,MS11-028,MS11-100,MS11-018,MS11-054,MS10-083,MS11-098,MS10-073,MS10-076,MS12-036,MS12-016,MS11-029,MS12-034,MS10-063,MS10-067,MS11-033,MS11-017,MS11-077,MS11-063,MS12-023,MS11-037,MS10-070,MS11-026,MS11-056,MS12-035,MS12-037,MS12-003,MS11-039,MS10-078,MS11-013,MS11-093,MS10-069,MS11-062,MS11-080,MS10-090,MS10-081,MS12-020,MS12-018,MS10-099,MS12-010,MS12-041,MS11-034,MS11-010,MS11-044,MS12-009,MS11-007,MS11-038,MS11-024,MS12-004,MS12-038,MS10-082,MS11-020,MS11-065,MS11-075,MS10-091,MS12-027,MS10-096,MS11-012,MS12-025,MS12-042,MS11-087,MS10-071,MS11-097,MS11-002,MS10-097,MS10-084,MS11-003,MS10-062,MS11-020</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-020,MS11-019,MS11-046,MS10-061,MS09-072,MS11-052,MS11-050,MS11-090,MS11-030,MS11-059,MS11-099,MS11-043,MS12-008,MS12-006,MS11-081,MS12-005,MS11-042,MS12-004,MS10-085,MS10-048,MS10-046,MS11-085,MS11-071,MS10-059,MS12-</td>
</tr>
<tr>
<td>IP Address</td>
<td>Microsoft Patch Reference</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>024,MS11-069,MS11-009,MS12-001,MS10-074,MS10-001,MS11-011,MS11-027,MS10-035,MS10-022,MS11-057,MS10-098,MS11-032,MS12-013,MS11-031,MS10-033,MS11-028,MS11-100,MS11-018,MS10-012,MS10-054,MS10-054,MS10-083,MS10-047,MS10-073,MS10-013,MS10-076,MS12-036,MS12-016,MS10-041,MS12-034,MS11-017,MS11-064,MS11-077,MS11-063,MS12-023,MS11-068,MS11-083,MS11-037,MS10-070,MS11-026,MS12-019,MS11-084,MS10-002,MS11-056,MS10-032,MS10-037,MS12-035,MS12-037,MS10-100,MS11-039,MS11-013,MS11-041,MS10-090,MS11-048,MS10-081,MS10-018,MS12-018,MS10-008,MS10-058,MS12-010,MS12-041,MS11-034,MS10-020,MS12-033,MS11-044,MS12-009,MS11-007,MS10-019,MS11-038,MS10-043,MS10-060,MS10-053,MS11-024,MS10-095,MS10-051,MS12-004,MS12-038,MS11-020,MS12-012,MS10-006,MS10-034,MS12-032,MS10-021,MS11-075,MS10-091,MS10-096,MS10-030,MS11-012,MS12-025,MS12-042,MS10-092,MS11-087,MS10-071,MS11-097,MS11-002,MS11-025,MS11-003,MS10-049,MS11-020,MS10-054,MS10-012,MS11-048</td>
<td></td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-027</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS10-041,MS12-035</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS11-078,MS12-016,MS11-039,MS12-034,MS12-008,MS12-024,MS12-013,MS12-036,MS12-023,MS12-008,MS11-035,MS12-035,MS12-037,MS12-020,MS12-018,MS12-010,MS12-041,MS12-033,MS12-009,MS12-038,MS12-032,MS12-025,MS12-042,MS11-025</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS11-078,MS12-016,MS11-039,MS12-034,MS12-008,MS12-024,MS12-013,MS12-036,MS12-023,MS12-008,MS11-035,MS12-035,MS12-037,MS12-020,MS12-018,MS12-010,MS12-041,MS12-033,MS12-009,MS12-038,MS12-032,MS12-025,MS12-042,MS11-025</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-020,MS12-008,MS11-066,MS12-024,MS11-069,MS11-078,MS12-013,MS11-028,MS11-100,MS12-036,MS12-016,MS12-034,MS12-030,MS12-023,MS10-070,MS12-019,MS12-035,MS12-037,MS11-039,MS12-020,MS12-018,MS12-010,MS12-041,MS12-033,MS11-044,MS12-009,MS12-038,MS12-012,MS12-032,MS12-027,MS12-025,MS12-042,MS11-025</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS11-069,MS11-078,MS11-028,MS11-100,MS12-036,MS12-016,MS12-035,MS12-037,MS11-039,MS12-041,MS11-044,MS12-038,MS12-025,MS12-042,MS11-025</td>
</tr>
</tbody>
</table>
| XXX.XXX.XXX.XXX     | MS12-020,MS11-090,MS11-099,MS12-008,MS11-081,MS12-005,MS11-085,MS11-071,MS12-024,MS11-069,MS12-001,MS11-078,MS12-013,MS11-028,MS11-100,MS12-036,MS12-016,MS12-034,MS11-077,MS12-023,MS11-083,MS12-019,MS11-084,MS12-035,MS12-037,MS11-039,MS12-020,MS12-018,MS12-010,MS12-041,MS12-033,MS11-044,MS12-009,MS12-004,MS12-038,MS12-
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Microsoft Patch Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>012,MS12-032,MS11-075,MS12-025,MS12-042,MS11-087,MS11-097,MS11-025</td>
<td></td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-034,MS12-036,MS12-035,MS12-037,MS11-058,MS12-041,MS12-033,MS11-095,MS12-038,MS12-032,MS12-017,MS12-025,MS12-042,MS11-086,MS11-058</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS11-090,MS11-099,MS12-008,MS11-081,MS12-005,MS11-085,MS12-024,MS12-001,MS11-078,MS12-013,MS11-100,MS12-036,MS12-016,MS12-034,MS11-077,MS12-023,MS11-083,MS09-035,MS12-019,MS11-084,MS12-035,MS12-037,MS12-020,MS12-018,MS12-010,MS12-041,MS12-033,MS12-009,MS12-004,MS12-038,MS12-012,MS12-032,MS11-075,MS12-025,MS12-042,MS11-087,MS11-097,MS11-025</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-020,MS11-046,MS11-052,MS11-050,MS11-090,MS11-099,MS11-043,MS12-008,MS12-006,MS11-081,MS12-005,MS11-042,MS11-085,MS11-071,MS12-024,MS11-069,MS12-001,MS11-078,MS10-022,MS11-057,MS12-013,MS11-031,MS11-100,MS11-018,MS11-054,MS11-098,MS12-036,MS12-016,MS12-034,MS11-064,MS11-077,MS11-063,MS12-023,MS11-068,MS11-083,MS11-037,MS10-070,MS12-019,MS11-056,MS12-035,MS12-037,MS12-003,MS11-039,MS11-048,MS12-020,MS12-018,MS12-010,MS12-041,MS12-033,MS11-044,MS09-045,MS11-038,MS12-004,MS12-038,MS12-012,MS12-032,MS11-075,MS12-027,MS12-025,MS11-087,MS11-025,MS11-048</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS12-020,MS10-065,MS11-019,MS11-046,MS11-052,MS11-050,MS11-090,MS11-099,MS11-030,MS11-059,MS11-099,MS11-043,MS12-008,MS12-006,MS11-081,MS12-005,MS11-042,MS11-085,MS11-071,MS12-024,MS11-069,MS12-001,MS11-078,MS11-011,MS11-027,MS11-057,MS11-032,MS12-013,MS11-089,MS11-031,MS11-028,MS11-100,MS11-018,MS11-054,MS12-036,MS12-016,MS11-021,MS11-072,MS11-045,MS12-034,MS12-030,MS11-073,MS11-017,MS11-064,MS11-077,MS11-063,MS12-023,MS11-068,MS11-083,MS11-037,MS11-026,MS12-019,MS11-084,MS11-056,MS12-035,MS12-037,MS11-039,MS11-013,MS11-041,MS11-048,MS12-020,MS12-018,MS12-010,MS12-041,MS11-034,MS12-033,MS11-044,MS11-009,MS11-007,MS11-038,MS11-024,MS12-004,MS12-038,MS11-020,MS12-012,MS12-032,MS11-075,MS12-027,MS11-012,MS12-025,MS12-042,MS11-087,MS11-097,MS11-025,MS11-003,MS11-020,MS11-048</td>
</tr>
<tr>
<td>XXX.XXX.XXX.XXX</td>
<td>MS11-019,MS11-046,MS11-052,MS11-050,MS11-090,MS11-030,MS11-059,MS11-099,MS11-043,MS12-008,MS12-006,MS11-081,MS12-005,MS11-042,MS11-085,MS11-024,MS11-069,MS12-001,MS11-078,MS11-011,MS11-054,MS11-085,MS11-071,MS12-023,MS11-068,MS11-083,MS11-037,MS11-026,MS11-019,MS11-084,MS11-056,MS12-035,MS12-037,MS11-039,MS11-013,MS11-041,MS11-048,MS12-020,MS12-018,MS12-010,MS12-041,MS11-034,MS12-033,MS11-044,MS11-009,MS11-007,MS11-038,MS11-024,MS12-004,MS12-038,MS11-020,MS12-012,MS12-032,MS11-075,MS12-027,MS11-012,MS12-025,MS12-042,MS11-087,MS11-097,MS11-025,MS11-003,MS11-020,MS11-048</td>
</tr>
</tbody>
</table>
### Recommendation:

Management should ensure that procedures are in place and followed to timely apply software patches to all servers and workstations. Additionally, various Microsoft and third-party software packages are available to help organizations manage the timely patching of their servers and workstations. If existing procedures do not efficiently result in patched servers, management should assess the need to implement a patch management software solution.

### Status:

Mark Babin began the process of updating all of the servers through Microsoft Automatic Updates while we were on-site and had scheduled ongoing updates to occur every Friday.

### Management Response:

The patches have been installed. Our current maintenance plan for patches is on a monthly basis. Some of the general servers have been configured for automatic updates weekly.

### Due Date:

Completed
F. ACCESS WITH DEFAULT CREDENTIALS—NEC UNIVERGE UM8000

Relative Risk: Medium
Resolution Level of Difficulty: Medium

Finding:

The Web application (Port 443) at address XXX.XXX.XXX.XXX was accessible using default login credentials (i.e., login $nec and no password). This access allowed us to make changes to the default voicemail box for the NEC phone system:

![Screen capture of NEC UNIVERGE UM8000]

Recommendation:

We recommend working with the vendor and reviewing this server for content. The vendor should both disable the default username and password and implement usernames and passwords in line with FWCJUA information security policies.

Management Response:

We will contact the vendor to see if they can implement any changes or change passwords.

Responsible Party: Marc Babin, IS Manager

Due Date: Completed

G. SERVER MESSAGE BLOCK (SMB) NULL SESSION AUTHENTICATION

Relative Risk: Medium
Resolution Level of Difficulty: Low

Finding:
The servers at addresses XXX.XXX.XXX.XXX, XXX.XXX.XXX.XXX, XXX.XXX.XXX.XXX and XXX.XXX.XXX.XXX are running Microsoft Windows 2003 server. It is possible to log into the SMB session on TCP Port 445 using a NULL session (i.e., with no login or password).

**Recommendation:**

We recommend that FWCJUA apply the following registry changes to these servers to mitigate this risk:

```
"HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess =1
Remove BROWSER from :
HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes
Reboot once the registry changes are complete."
```

**Management Response:**

The registry changes have been made on the 2003 servers. All except one are to be decommissioned by end of the year.

**Responsible Party:** Marc Babin, IS Manager

**Due Date:** Completed
VI. WIRELESS NETWORK SECURITY FINDINGS AND RECOMMENDATIONS

A. WIRELESS NETWORK ENCRYPTION

Our review did not identify any significant security issues that could cause operational or security issues with your wireless network.

Observation:

FWCJUA utilizes the SonicWall SonicPoint for configuration and implementation of wireless networking throughout the main office building holding corporate, information technology services, human resources, payroll and internal audit departments. Once connected, users on the corporate wireless network must authenticate to a terminal services server with their Active Directory domain account to access corporate applications. A second wireless network was constructed using the SonicWall Virtual Access Point (VAP) feature set on the SonicPoint. This VAP is utilized for guest access to the Internet.

Corporate access is configured using Wi-Fi Protected Access 2- (WPA2-) preshared key (PSK) authentication and encryption method. Guest access is configured utilizing WPA-PSK authentication encryption. Users must be supplied with the requisite PSK for access to either network. These keys are different for each network.

McGladrey found that very little broadband traffic is utilized for the wireless network. Due to this, within the time frame for the engagement, it would be unlikely that enough traffic could be collected to break the WPA or WPA2 encryption algorithm.

B. ENCRYPTION KEY

Observation:

We attempted to decrypt the key during our on-site visit and were not successful.

C. GEOGRAPHIC COVERAGE

Observation:

Spread Spectrum radio’s propagation pattern when used with an omni-directional antennae tends to be a flat donut-like pattern and can often spread into public areas. We used a laptop equipped with the built-in Intel Centrino Advanced-N wireless adapter to footprint the coverage area of the access points.
The coverage pattern is as follows:

- We were able to receive useable signals in most areas of the parking lot and, the closer to the building, the better the signal. The best area to intercept the signal was in the parking lot directly in front of the building, as we were able to identify both of FWCJUA’s wireless access points.

- Based on our readings, it would be logical to assume that a high-gain directional antennae would be effective in intercepting the signal well beyond the parking lot limits.

- It appears as though the current placement of access points provides adequate coverage of the main facility and beyond. There is some risk to the wireless network in that the signal extends well beyond the walls of the facility into the parking lots. Current efforts to manage this risk include:
  - Implementation of WPA and WPA2
  - Implementation of separate virtual LAN (virtual LAN2) for wireless access point to firewall
  - IP address filtering implemented within the firewall to permit only legitimate handheld devices
  - Positioning of the Web server in the demilitarized zone with strict firewall filtering protects the Web server from unauthorized attempts
D. **Encryption Level**

*Observation:*

WPA2 and WPA are being utilized to negotiate keys for encryption.

E. **Access Point Hardware Implemented**

*Observation:*

One SonicWall SonicPoint access point and a VAP have been deployed.

F. **Access Point Configuration**

*Observation:*

- Web administration is permitted, but is limited by login and password.
- Documentation of the configuration was found to be accurate.
VII. FIREWALL SECURITY OBSERVATIONS

McGladrey reviewed the firewall rule sets and configurations on the SonicWall firewalls (TZ 0017C5987C14 and 0017C51A28C8). The review included common misconfigurations and the state of established rules.

A. EXTENSIVE OPEN PORTS—EXTERNAL INTERFACE

Relative Risk: High
Resolution Level of Difficulty: Medium

Finding:

Both of the firewalls’ external interfaces have TCP Ports 28000 through 30000 open to any source address on the Internet. These ports were configured for one of FWCJUA’s larger service providers to make Secure File Transfer Protocol transfers to FWCJUA on a random port within this range. An attacker could leverage access to these ports to attempt access to the internal network.

Recommendation:

We recommend limiting access to these ports to only the service provider’s Internet IP subnet(s).

Status: This finding was remediated while we were on-site.
VIII. EXHIBITS

A. TOOLS UTILIZED

The following is a list of the tools available to McGladrey LLP’s security consultants to assess an organization’s data network. McGladrey may not use all of these tools during an assessment. This list is provided to illustrate the variety and breadth of tools that can be used by McGladrey’s security consultants during network security reviews.

Commercial Tools

- Tenable Network Security—Nessus Scanner with ProfessionalFeed
- IBM’s AppScan—used for Internet application security assessments
- Application Security Inc.’s AppDetective
- CACE Technologies’ AirPcap
- Sandstorm Enterprises’ PhoneSweep
- Athena Security, Inc.’s FirePAC and Verify—used for the analysis of firewalls and network devices
- Qualys—vulnerability scanning appliance
- Other commercial network security testing tools

Publicly Available Tools

- Telnet
- SuperScan
- Sam Spade
- NSLookup
- NetStumbler
- Wireshark
- Kismet
- Air Snort and other wireless tools
- Other public domain tools and scripts from a variety of sources
B. Footprinting Information

“Footprinting” is the term used to describe the process of information gathering to identify all aspects of an organization’s security posture. By using a combination of tools and techniques, an attacker can take an unknown network and reduce it to a specific range of domain names, network blocks and individual IP addresses of systems directly connected to the Internet. By using various methods, we were able to develop the footprint for FWCJUA. This information is included as an electronic file accompanying this report.

C. Enumeration Information

“Enumeration” is the term used to describe the process of extracting valid user/customer accounts. By using a combination of tools and techniques, we attempt to extract user/customer account information. These activities are intrusive in nature and involve creating active connections to systems. The following are the results of our enumeration activities. For brevity, we have not included the results of every enumeration attempt conducted unless those activities generated different results.

We were not able to penetrate FWCJUA’s network and obtain any user/customer account information.

D. Vulnerability Report Key

The following provides a general description of the information provided by the various commercial tools used to assess FWCJUA’s external and/or internal network security.

The reports contained in the following sections are the raw, unanalyzed results of the automated security assessment tools. FWCJUA’s management and technical personnel should refer to Sections IV and V of this report for our analysis and prioritization of the information contained in the following sections.

Session Information

This documents the information regarding the configuration of the application used to conduct the network security review. Key information available includes the policy used and time the assessment was started and ended.

Service Details

This section of the report provides information regarding the “well known” services (TCP/UDP Ports 1 – 1023) found running on these systems evaluated. Information provided includes the port number, type of port (TCP, UDP), service name and a short description of the service.

Banner Details

This section of the report provides additional information regarding any banner information that was retrieved when the target system was contacted over a particular service. Information provided includes the type of banner and the banner text received.
Others

This section contains any additional information retrieved by the various tests that were performed. Information available is free format and will vary depending on the types of services encountered and their responses to requests.

Vulnerability Details

This section of the report documents the vulnerabilities identified during the session. Each vulnerability identified during the session is assigned a severity by an icon indicating high, medium or low, a short description of the vulnerability, a discussion of the vulnerability (i.e., how it works, conditions under which it works, etc.), and a discussion of how to correct or remedy, if possible, the vulnerability.

Vulnerabilities assigned a high level of severity should be addressed immediately as they can be used to compromise the device or cause the device to become inoperative. Vulnerabilities assigned a medium level of severity may also be used to compromise the device or can be used in conjunction with other vulnerabilities to compromise the device or otherwise make the device inoperative. Vulnerabilities assigned a low level of severity are vulnerabilities that provide information that combined with other information or vulnerabilities allow unauthorized persons to improve their chances of compromising the device or making the device inoperative.

E. EXTERNAL VULNERABILITY REPORTS

If the volume of external vulnerability reports is small, the hard copy of the reports is included here. Otherwise, the reports are accompanying this report in electronic format.

F. INTERNAL VULNERABILITY REPORTS

If the volume of internal vulnerability reports is small, the hard copy of the reports is included here. Otherwise, the reports are accompanying this report in electronic format.
PRELIMINARY 2013 BUSINESS PLAN & FORECAST

The Operations Committee’s shall consider staff’s preliminary draft of the 2013 Business Plan & Forecast, including the projected 2013 capital expenditures.

Of note, the preliminary 2013 Business Plan & Forecast currently contemplates the following:

1. The restatement of the FWCJUA’s objectives:
   a. Delete managing the Subplan D deficit given by year-end 2012, the FWCJUA will have closed all Subplan D claims and finalized the deficit such that any excess State funding may be returned to the State no later than 1Q 2013.
   b. Add maintaining the MAP program to the objectives as it is a goal of the FWCJUA’s mission.

2. Staff’s $30 million Written Premium projection for 2013, which will also be considered by the Reinsurance and Rates & Forms Committees prior to the September 12th Board meeting.

3. The continued use of contracted attorneys in lieu of in-house attorneys for legal services;
   a. Tom Maida, of Foley & Lardner, will continue to be engaged as the General Counsel with a fee increase from $157,000 to $167,000. The fees have not changed since January 1, 2009, and the proposed increase is less than the CPI inflation (cost of living) increase since that time.
   b. Steve Coonrod, of McConnaughhay, Duffy, Coonrod, Pope & Weaver, will continue to be engaged as the Claims Litigation Manager with a fee increase from $175/hour to $185/hour. The fees have not changed since January 1, 2008, and the proposed increase is less than the CPI inflation (cost of living) increase since that time.

4. The discontinuance of an annual outsourced IT audit recognizing that future IT audits may be requisitioned when significant reconfigurations or overhauls to the infrastructure necessitate.

5. Competitive solicitations for the selection of a policy administration/managed care service provider, reinsurance intermediary, and actuary.

With regard to item 3 above, the FWCJUA currently contracts directly for general counsel services as well as claim litigation management services. The General Counsel has provided assistance through his firm on a multitude of issues over the years; and given the wide range of expertise at the General Counsel’s firm, it has consistently been the Board’s position that the FWCJUA would not be able to cost effectively hire an in-house attorney to perform these services let alone keep the individual busy on a full-time basis. The Claims Litigation Manager supervises claims litigation and advises as to litigation issues. These duties include review of ongoing workers compensation, employment liability and other litigation, development of guidelines for file review, development of standards for defense counsel utilized by the FWCJUA, and providing updates as to legislative and other relevant legal developments. Responsibilities may also include representing the FWCJUA in legal proceedings in coordination with General Counsel. Again, it has been the Board’s position that it would not be cost effective to hire an in-house attorney to provide these services because of the very limited time we anticipate utilizing the services. In September 2011, the Board agreed that the services for General Counsel and claims litigation management should continue to be performed by contracted attorneys rather than in-house attorneys, and also endorsed continuing the relationship with both of our current outside attorneys.

Attached for discussion purposes is a copy of the Preliminary 2013 Business Plan & Forecast, including capital expenditures, and a summary of services provided by the FWCJUA’s General Counsel. All new key activities in the proposed preliminary 2013 Business Plan & Forecast have been identified with red underscore for ease of reference. It is staff’s intent to finalize this working draft of the 2013 Business Plan & Forecast to include capital expenditures over the next several months so the Committee can finalize it and recommend it for approval at the December Board meeting.

The Committee shall provide comments with regard to the preliminary 2013 Business Plan & Forecast, including capital expenditures.
INTRODUCTION
Following is the FWCJUA business plan for 2013 defining our objectives and key activities. We are confident that in 2013 we will meet our obligations to the legislature and our policyholders through our results-oriented, bottom-line focus. We shall continue to concentrate on the critical activities that ensure continued success - managing expenses, properly pricing the product and providing creative solutions to problems generated by a constantly changing market.

MISSION
As the Board of Governors of the FWCJUA, we have been charged with the duty of administering the Florida Workers' Compensation residual market mechanism. In fulfilling that obligation, our goals are:

To provide workers’ compensation and employer's liability insurance to employers who are required to maintain such coverage by law but are unable to procure it in the voluntary market and who are willing to implement reasonable loss prevention programs to provide safe work places;

To ensure that policyholders and claimants receive quality service;

To provide coverage and service efficiently and to establish rates that are actuarially sound and reasonably expected to ensure the ongoing solvency of the residual market mechanism without future policyholder assessments;

To establish and aggressively pursue programs designed to assist applicants and insureds of the residual market mechanism to obtain coverage in the voluntary market; and

To promote safety in the work place through the aggressive pursuit of safety programs for insureds of the residual market mechanism.

OBJECTIVES
Our 2013 objectives are:

1. Maintain rate adequacy.
2. Minimize the operating loss.
3. Maintain solvency without an FWCJUA policyholder assessment provided rate adequacy exists.
4. Pursue sound investments.
5. Manage uncollectible premiums within acceptable limits.
6. Maintain a dynamic, responsive organization capable of responding to market fluctuations in a timely manner.
7. Implement a policyholder return of premium dividend, if declared.
8. Implement an assessment, if one becomes necessary.
9. Promote loss prevention and safety in the workplace of our policyholders.
10. Maintain a market assistance plan that provides access to and assists in the placement of voluntary market coverage for FWCJUA applicants and policyholders.

KEY ACTIVITIES/SUCCESS FACTORS
Our 2013 objectives are supported by the key activities (success factors) defined on the following pages.

1. MAINTAIN RATE ADEQUACY.
   a) Assure rate adequacy through conducting semiannual rate adequacy analyses culminating in the implementation, as appropriate, of revised rates and/or rating plans consistent with the FWCJUA’s mission and statutory charge to provide workers’ compensation and employer’s liability coverage to those unable to obtain it in the voluntary market.

2. MINIMIZE THE OPERATING LOSS.
   a) Monitor the IRS progress on the development of regulation or any other published guidance with regard to the topic of what constitutes an integral part of a state, local, or Indian tribal government
PRELIMINARY FWCJUA 2013 BUSINESS PLAN

for federal income tax purposes such that a Private Letter Ruling may be further pursued as appropriate.

b) The operation will continue to concentrate on underwriting - determination of actual exposures and proper pricing, prompt policy issuance, premium collection, fraud prevention, market assistance, and evaluation of current performance standards.

(1) Analyze the composition and experience of new and renewal business, and modify as appropriate, underwriting, collections and fraud prevention practices and procedures to ensure that existing programs realize maximum effectiveness and efficiencies. Develop new practices, procedures or programs as analysis dictates.

(2) Monitor the number of accounts exceeding $300K in premium to determine if there is sufficient increased activity to warrant further consideration of a loss sensitive rating plan. As directed by Committee

c) Ensure that the financial audit for 2012 is completed no later than June 1, 2013.

d) Satisfy any recommendations presented in the Auditor’s Letter to Management no later than June 1, 2013.

e) Manage to the G&A budget.

f) Prepare and file the FWCJUA Annual Financial Statement no later than March 1, 2013 and the Quarterly Financial Statements no later than May 15, August 15 and November 15, 2013.

g) Prior to July 1\textsuperscript{st}, notify the Office of Insurance Regulation of the amount of the FWCJUA’s gross written premiums for the preceding calendar year pursuant to section 440.51(14), Florida Statutes. (Whenever the plan's gross written premiums reported to the Office are less than $30 million, the Office shall transfer to the plan, subject to appropriation by the Legislature, an amount not to exceed the plan’s fixed administrative expenses for the preceding calendar year, subject to a maximum of $750,000)

3. MAINTAIN SOLVENCY WITHOUT AN FWCJUA POLICYHOLDER ASSESSMENT PROVIDED RATE ADEQUACY EXISTS.

a) Manage the Projection Models and financial reports by subplan and tier to anticipate potential solvency problems and recommend courses of action to the Board.

b) Ensure that the Statement of Actuarial Opinion for 2012 is completed no later than April 1, 2013.

c) Conduct a reserve analysis on the loss liabilities of the FWCJUA to include case reserves and IBNR losses, the adequacy of case reserves to pay reported open claims; and a comparison of assets and liabilities with a recommendation by subplan as to the necessity of an assessment to fund outstanding liabilities.

d) Review the existing reinsurance program early in the renewal cycle to ensure it meets both current and anticipated needs; release the renewal submission early in order to review additional options; and negotiate an appropriate renewal.

e) From a strategic perspective, review different types of reinsurance programs that are available and recommend any strategic perspective alternatives to the current casualty-based program.

f) Conduct a risk assumption analysis in conjunction with either the reinsurance intermediary’s actuary or the FWCJUA's consulting actuary that describes how much risk the FWCJUA could assume at various attachment points and the implications of that risk assumption.

g) Ensure timely and accurate reporting to the reinsurers with full disclosure of large and/or serious injuries.

h) Continue the proactive role in monitoring serious injury claims, the regular, formal review of “old” and large open claims and the requirement for settlement authorization for amounts of $50,000 or greater.

i) If a deficit is recognized at the 2012 audit, a program to eliminate the deficit will be developed and filed with OIR within 90 days.

j) Monitor the 1994 – 1999 LPT transaction to determine the status of the restrictive surplus and the status of the aggregate limit.

k) Prepare and file the Management Discussion and Analysis no later than April 1, 2013.

4. PURSUE SOUND INVESTMENTS.

a) Evaluate short-term and intermediate cash flow needs according to the cash management policy along with current economic conditions and modify the investment strategy as warranted.

b) Evaluate, direct and monitor the performance of the investment manager to ensure that performance is at or above market benchmark returns.
c) Conduct quarterly Investment Committee meetings as scheduled to monitor investment compliance, as necessary.

5. MANAGE UNCOLLECTIBLE PREMIUM WITHIN ACCEPTABLE LIMITS.
   a. Evaluate and monitor the collection activity by subplan and tier to ensure that uncollectible premium is held to or below our average policy year uncollectible premium for policy years 1994 through 2010 of XX% as of 12/31/12.
   b. Identify the leading drivers of uncollectible premium and adjust collection programs to enhance collection efforts.

6. MAINTAIN A DYNAMIC, RESPONSIVE ORGANIZATION CAPABLE OF RESPONDING TO MARKET FLUCTUATIONS IN A TIMELY MANNER.
   a. Evaluate process for data transfers to and from Service Providers and improve ongoing reliability, security and redundancy of the data exchange.
   b. Upgrade the FLARE and Tropics reporting platform to incorporate ad-hoc and dynamic report capability.
   c. Ensure that the FWCJUA website is “real-time” with respect to: 1) rules; 2) procedures; 3) applications; 4) forms; 5) rates; 6) the premium calculator; 7) the “authorized agency/producer” locator; 8) answers to FAQ’s; 9) MAP reports; and 9) general information.
   d. Ensure that new application submissions are reviewed and responded to within 1 business day.
   e. Create internal IT Audit procedures for systems and security to be performed and documented at least twice yearly. As directed by Committee
   f. Secure vendor for alarm system and evaluate current solution.
   g. Confirm the Financial Auditor for the 2013 year-end audit.
   h. Conduct an RFQ to engage a reinsurance intermediary for the placement of at least the 2014 reinsurance program with the selection to be made by the end of 1Q. As directed by Committee
   i. Conduct an RFP to engage an independent consulting actuary to provide reserve and ratemaking services no later than end of 2Q. As directed by Committee
   j. Conduct an RFP to engage a policy administration/managed care service provider no later than end of 2Q to issue policies with effective dates of January 1, 2014 and subsequent.
   k. Re-engage NCCI as the statistical agent for the FWCJUA by November 18, 2013.
   l. Conduct an annual audit, to include a review of its Disaster Recovery Plan, Document Retention Policy, and Antifraud Plan, as well as quarterly reviews of the policy administration/managed care service provider’s performance to ensure adherence to FWCJUA rules and service standards.
   n. File the Records Management Compliance Statement form in 4Q identifying the FWCJUA’s compliance with records management laws and rules and provide updated agency and Records Management Liaison Officer information.
   o. Explore and implement disaster recovery initiatives as deemed appropriate by the Board.
   p. Actively pursue Producer, Employer and Claimant fraud through conducting cooperative investigation with the Service Provider; preparing and submitting fraud reports; and participating in the state’s prosecution activities.
   q. Support the Division of Compliance’s monitoring of FWCJUA employers who are cancelled or do not renew coverage and also applicants who do not purchase FWCJUA coverage.
   r. Prepare and submit, at least quarterly, to the Commission on Ethics a list of names of the senior managers, officers, and members of the Board who are subject to the public disclosure requirements under section 112.3145, Florida Statutes, with the first list submitted no later than March 31, 2013.
   s. Add WebTropics & Tropics Application Enhancements when and if projects identified.

7. IMPLEMENT A POLICYHOLDER RETURN OF PREMIUM DIVIDEND, IF DECLARED.
   a. Compile the financial information for the 2006 policyholders as well as the methodology analysis and expense calculation exhibits for Board consideration in 2Q.
   b. Issue any required dividend checks no later than August 1, 2013.

8. IMPLEMENT AN ASSESSMENT, IF ONE BECOMES NECESSARY.
   a) Continue to explore alternative ways to minimize assessment potential.
9. PROMOTE LOSS PREVENTION AND SAFETY IN THE WORKPLACE OF OUR POLICYHOLDERS.
   a) Conduct causes of loss analyses and modify the safety program as warranted to satisfy any deficiencies given our emerging book of business.
   b) Explore “alternative” methods and techniques for accepting and using safety programs and make appropriate recommendations to the Safety Committee.

10. MAINTAIN A MARKET ASSISTANCE PLAN THAT PROVIDES ACCESS TO AND ASSISTS IN THE PLACEMENT OF VOLUNTARY MARKET COVERAGE FOR FWCJUA APPLICANTS AND POLICYHOLDERS.
    a) Evaluate the effectiveness of MAP and make appropriate recommendations to the MAP Committee.
**Florida Workers’ Compensation Joint Underwriting Association, Inc.**

**Annual Budget & Forecast comparison**

**For the Twelve Months Ending December 31, 2012 & 2013**

<table>
<thead>
<tr>
<th>2012 Budget</th>
<th>2013 Budget</th>
<th>% Change</th>
<th>2012 Budget forecast</th>
</tr>
</thead>
</table>

### REVENUE:

- **Direct written premium (new & renewals with PY 2010)**: $16,250,000, $9,000,000, 90.32%
- **EBUB Written premium**: (78,309), -
- **Direct written premium (prior years’ adjustments)**: (500,000), (927,480), 85.50%
- **Direct earned premium (new & renewals with PY 2010)**: 7,966,982, 14,372,726, 80.40%
- **EBUB Eared premium**: (78,309), -
- **Direct earned premium (prior years’ adjustments & UEP)**: 4,752,154, 8,283,018, 73.21%
- **Reinsurance premium**: 2,084,484, 3,704,214, 77.70%
- **Net earned premium**: 10,586,342, 18,951,530, 79.02%

**Investment income incl. unrealized gains/losses**: 1,200,000, 1,750,000, 45.83%

### OPERATING EXPENSES:

- **Bad debt write-off - 4.5% Earned**: 573,711, 1,019,508, 77.70%
- **Ceded reinsurance recoverables**: 962,855, 1,712,669, 77.87%

**Total Revenue**: 11,822,822, 20,721,530, 75.27%

### GENERAL & ADMINISTRATIVE EXPENSES:

- **Bad debt write off - (suspected fraud adj.)**: -
- **Net loss & LAE incurred**: 5,868,111, 11,463,976, 95.36%

**Operating Expenses**: 10,586,342, 18,951,530, 79.02%

### TOTAL PERSONNEL:

- **Total Personnel**: 447,791, 551,895, 23.25%

### PERSONNEL:

- **General**: 175,712, 176,360, 0.37%
- **Bank charges**: 1,000, 1,000, 0.00%
- **Telecommunications**: 52,922, 50,870, -3.88%
- **Insurance - BES/GLC/WC&D&O**: 82,065, 84,870, 3.86%
- **Licenses and fees**: 1,185, 1,158, 0.00%
- **Office equipment and supplies**: 106,449, 108,329, 1.77%
- **Disaster Recovery Plan Maintenance**: 68,178, 68,178, 0.00%
- **Utilities**: 12,000, 9,600, -20.00%
- **Depreciation/amortization**: 313,706, 93,835, -70.09%

**Total General**: 818,710, 601,724, -26.50%

### PERSONNEL:

- **Compensation**: 1,091,352, 1,114,159, 2.09%
- **Benefits**: 209,001, 195,837, -6.30%
- **Payroll taxes**: 78,965, 79,754, 1.00%
- **Employee recruitment/training/education**: 7,800, 3,000, -61.54%

**Total Personnel**: 1,387,118, 1,392,750, 0.41%

### TRAVEL & BUSINESS EXPENSES:

- **Travel - employees**: 15,000, 15,000, 0.00%
- **Travel - board/committee meetings**: 15,300, 15,300, 0.00%

**Total Travel and Business Expenses**: 30,300, 30,300, 0.00%

**Total General & Administrative Expenses**: 2,683,918, 2,576,669, -4.00%

### KEY INITIATIVE EXPENSES:

- **Ligation**: 60,000, 60,000, 0.00%
- **Legislative initiatives**: -
- **Legal - Special Projects**: -
- **Second rate filings**: -

**Total Key Initiative Expenses**: 60,000, 60,000, 0.00%

**Total G&A and Key Initiatives**: 2,743,918, 2,636,669, -3.91%

**Total All Expenses**: 12,283,556, 20,256,990, 64.91%

**Gain/(Loss) Before policyholder dividends**: (460,733), 464,546, -200.83%
Florida Workers' Compensation Joint Underwriting Association, Inc.
Budgeted Capital Expenditures
For Year Ending December 31, 2013

<table>
<thead>
<tr>
<th>Hardware</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UPS - battery replacement</td>
<td>6,000</td>
</tr>
<tr>
<td>Laptops as replacement for thin Clients (11)</td>
<td>13,200</td>
</tr>
<tr>
<td>Scanner replacement - only if needed</td>
<td>7,500</td>
</tr>
<tr>
<td>Alarm System - project to find vendor &amp; upgrade</td>
<td>5,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning software/tools - for internal audit.</td>
<td>2,000</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>33,700</strong></td>
</tr>
</tbody>
</table>

Annual depreciation / amortization  11,233
X 75% assuming 4/1/2012 avg implementation  8,425
X 75% assuming 4/1/2012 avg implementation  6,319
Tom Maida, of the law firm of Foley & Lardner LLP (“Foley”), has acted as the FWCJUA’s General Counsel since the organization’s inception in 1994. In addition to personally providing legal services to the FWCJUA, Mr. Maida also supervises other attorney’s in his firm who provide legal counsel or representation to the organization. The specific services rendered by the General Counsel and his firm are performed under the direction and supervision of the Executive Director. Pursuant to the 2012 engagement agreement for legal services, the FWCJUA pays Foley an annual flat fee of $157,000 for general counsel services. The annual fee is payable in 12 monthly installments of $13,083.33 each. Further, the General Counsel's fees have remained at there current levels since January 1, 2009.

The FWCJUA is required by law to engage in a competitive bidding process to select some of its vendors. By law, however, the FWCJUA is not required to use a competitive bidding process to select its General Counsel. Similarly, state agencies are not required to use competitive bidding to select their outside law firms. The FWCJUA’s Board is required to determine whether it is more cost-effective and in the best interests of the organization to use legal services provided by in-house attorneys employed by the FWCJUA rather than contracting with outside counsel. At its September 27, 2011 meeting, the Board determined it was more cost-effective and in the best interests of the FWCJUA to continue to engage Mr. Maida as its outside General Counsel rather than employ an in-house General Counsel. The Operations Committee will reconsider this matter as it formulates the 2013 Business Plan & Forecast on August 29, 2012.

The specific legal tasks assigned to the General Counsel by the Executive Director vary based upon the needs of the FWCJUA and the issues faced by the organization from time to time. In general, however, the General Counsel is routinely expected to perform such services as:

- Act as the FWCJUA’s counsel and chief legal adviser
- Provide legal advice to the Board, the Board’s committees, and the Executive Staff regarding the performance of their duties and responsibilities
- Provide corporate governance compliance counsel
- Provide anti-trust compliance counsel
- Provide advice and counsel with respect to compliance with the Florida Public Records Law
- Provide advice and counsel with respect to compliance with Florida Government-in-the Sunshine laws
- Provide advice and counsel regarding compliance with state financial disclosure and ethics requirements
- Advise the FWCJUA with respect to insurance regulatory matters, including rate and forms filings, and represent the FWCJUA before the Florida Office of Insurance Regulation
- Advise the staff in connection with requests for proposals from potential vendors and, where necessary, assist the staff in the preparation of RFPs
- Prepare vendor contracts, and in other instances provide legal review of contracts prepared by vendors
SUMMARY OF SERVICES PROVIDED BY THE FWCJUA’S GENERAL COUNSEL

- Advise the staff in connection with various policyholder issues, to include policyholder return of premium dividend matters
- Advise the Board and the Executive Director regarding labor and employment issues
- Advise the Board and staff in connection with various Florida constitutional law issues
- Provide counsel regarding tax issues which affect the FWCJUA’s federal tax status, as well as provide counsel to the staff on matters of Florida tax law
- Attend all meetings of the Board and its committees
- Review all agenda materials in advance of Board or committee meetings
- Respond to any legal questions posed by the Board, its committees or the Executive Staff

In addition to providing the foregoing services, Foley also monitors relevant activity in the Florida Legislature and regularly reports to the Board and the Executive Staff on legislative developments which may be of interest to the organization. The General Counsel also acts as the FWCJUA’s liaison to the Legislature and responds to inquiries from legislative staff. These legislative monitoring and liaison services are included in the scope of services provided by the General Counsel, and the FWCJUA is not charged any additional fee for these services.

The General Counsel does not handle or supervise the FWCJUA’s routine litigation matters, such as claims litigation and collections litigation. Claims defense litigation is assigned to other law firms throughout the state and is supervised by the FWCJUA’s staff. The FWCJUA has also engaged the services of a law firm other than Foley to provide special claims counsel with respect to more sensitive claims or claims requiring special attention. The FWCJUA also engages separate collections counsel who also acts under the direction of the staff.

At the specific request of the Executive Director, Foley does, from time to time, represent the FWCJUA in connection with certain civil and administrative litigation. The civil litigation matters handled by Foley usual involve situations (1) where Foley is expected to quickly negotiate a settlement or obtain a relatively quick dismissal of a case, thereby resulting in cost savings to the FWCJUA or (2) where an important core principal is at issue and adverse results could have significant negative ramifications for the FWCJUA’s operations. In the administrative area, the Executive Director, from time to time, also specifically engages Foley to handle administrative appeals brought by policyholders before the Office of Insurance Regulation. The Executive Director believes Foley’s location in Tallahassee and its broad experience in handling policyholder appeals results in the most efficient use of the organization’s resources.
POLICY ADMINISTRATION/MANAGED CARE SERVICE PROVIDER ENGAGEMENT

The Operations Committee will provide direction to staff on its proposed service provider selection process and timeline for securing policy administration and managed care services beyond December 31, 2013.

Following are the decision points to be considered:

**Type of Service Provider Sought:**
1. Policy administration services including managed care proposed by a single entity; or
2. Policy administration services with a managed care arrangement proposed by a partnership/joint venture.
3. No stand alone proposals will be accepted.

**Number of Service Providers Sought:**
1. One (Alternative: maximum of two)

**Engagement Period:**
1. Five years, for policies issued with effective dates of January 1, 2014 through December 31, 2018 (traditionally have contracted for a three year engagement period)
2. Option of 2 one-year extensions

**Minimum Requirements to Bid:**
1. An insurer authorized to write workers’ compensation and employer’s liability insurance in Florida, pursuant to Chapter 624, Florida Statutes, whether domestic or foreign; or a commercial self-insurance fund organized pursuant to section 624.462, Florida Statutes; or a group self-insurance fund authorized by section 624.4621, Florida Statutes; or an assessable mutual insurer authorized by 628.6011, Florida Statutes; or a management company, service company or administrator authorized by the Florida Office of Insurance Regulation to provide workers compensation services to assessable mutual, commercial self-insurance funds, group self-insurance funds or individual self-insureds;
2. Five years experience in providing general policy administration services to workers compensation residual markets in the United States;
3. Five years experience in adjusting Florida workers compensation claims;
4. Provide, at a minimum, general policy administration services including, but not limited to, the issuance of policies and appropriate endorsements; premium billing and collection; auditing; claims management with managed care services, including, but not limited to, medical management and disability management; loss control and safety engineering; fraud investigation and prevention; financial and statistical data reporting; and customer satisfaction services, in a prompt, effective and efficient manner, as required by an in accordance with the procedures and standards of the FWCJUA;
5. Adjust claims out of a Florida office while providing policy administration services to the FWCJUA;
6. Provide managed care services including, but are not limited to, medical management and disability management. Claims administration services, which have historically been provided to the FWCJUA by the policy administration services vendors, may be provided by either vendor or a combination of both; and
7. Have the capacity and desire to handle 100% of the FWCJUA business (or at least 50% of the FWCJUA business recognizing that a maximum of two service providers may be selected).

**Service Fees:**
1. Must be quoted as a percent of collected written premium, excluding all written premium collected by the FWCJUA’s designated collection agent(s).

**Evaluation Process:**
1. The Evaluation Team will include the FWCJUA Executive Director, Operations Manager and Controller. The Evaluation Team will review and score the proposals utilizing the evaluation criteria set forth below, which may include conducting its own interviews and presenting its findings and recommendations to the Operations Committee. Other staff may also assist in the initial mandatory requirements review, contacting of references, or answering technical questions from the Evaluation Team. The Operations Committee shall then consider the Evaluation Team’s recommendation, which may include conducting its own interviews with some of the respondents, to formulate its recommendation to the Board as to its choice for policy
administration services including managed care. The Board shall then make the final determination.

### EVALUATION CRITERIA FOR THE FWCJUA RFP FOR POLICY ADMINISTRATION SERVICES INCLUDING MANAGED CARE

<table>
<thead>
<tr>
<th>MANDATORY DOCUMENTATION</th>
<th>Pass/Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Issuance &amp; Premium Collection</td>
<td>20</td>
</tr>
<tr>
<td>Premium Audit</td>
<td>10</td>
</tr>
<tr>
<td>Loss Control Services</td>
<td>10</td>
</tr>
<tr>
<td>Claims Administration</td>
<td>40</td>
</tr>
<tr>
<td>Managed Care</td>
<td>10</td>
</tr>
</tbody>
</table>

#### SCOPE OF SERVICES

- **Premium Audit**: 10
- **Loss Control Services**: 10
- **Claims Administration**: 40
- **Managed Care**: 10

#### COST OF SERVICES

<table>
<thead>
<tr>
<th></th>
<th>Pass/Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>100</td>
</tr>
</tbody>
</table>

**Timeline:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Issue RFP</td>
</tr>
<tr>
<td>2</td>
<td>Mandatory Bidders Conference</td>
</tr>
<tr>
<td>3</td>
<td>Deadline for Written Inquiries</td>
</tr>
<tr>
<td>4</td>
<td>Deadline for Responses to Written Inquiries Posted on FWCJUA Website</td>
</tr>
<tr>
<td>5</td>
<td>Deadline for Proposal Submissions</td>
</tr>
<tr>
<td>6</td>
<td>Interviews at FWCJUA office, if requested</td>
</tr>
<tr>
<td>7</td>
<td>Proposal Review Completed by Evaluation Team</td>
</tr>
<tr>
<td>8</td>
<td>Operations Committee Meeting</td>
</tr>
<tr>
<td>9</td>
<td>Anticipated Contract Award Date (Board Meeting)</td>
</tr>
<tr>
<td>10</td>
<td>Anticipated Contract Effective Date</td>
</tr>
<tr>
<td>11</td>
<td>Anticipated Contract Duration</td>
</tr>
</tbody>
</table>

Notice:

The RFP will be posted on the FWCJUA website on March 8th and notice of this posting will be published as follows:

1. March 8th in the Florida Administrative Weekly;
2. March 8th emails to FWCJUA Board, service providers and Interested parties; and
3. March 8th emails to NCCI’s list of multi-state residual market workers compensation service providers.

The award of a contract resulting from the RFP shall be based on the best proposal(s) received from the respondents meeting the mandatory requirements of the RFP who offer the lowest compensation requirements; the most cost effective administration for FWCJUA business; and the strongest emphasis on the reduction of operating losses. The FWCJUA shall reserve the right to decline to accept any or all RFP responses.

The Operations Committee will provide direction to staff on its proposed service provider selection process and timeline for securing policy administration and managed care services beyond December 31, 2013.
REPORT ON OPERATIONS

Highlights of operational objectives that have been addressed since the Board’s June 13th meeting include:

1. On June 18th, the FWCJUA filed its program to eliminate the 2011 Subplan “D” deficit with OIR.
2. On June 19th, June 21st, June 25th and August 7th, staff sent status updates to Aon Benfield on large loss serious injury claims in reply to inquiries received from reinsurers.
3. On June 21st, staff gave a brief presentation to FCCI’s Underwriting unit regarding the FWCJUA’s Market Assistance Plan (MAP), including the quote reporting mechanism and the pricing tool, all available for use on the FWCJUA’s website.
4. On June 25th, staff began testing the new web-based online Agency Authorization process to capture and save information directly into the Agency module of the Tropics Application system.
5. On June 25th, staff began to test the Phase 2 enhancements of WebTropics to help reduce the overall time for the Producer to submit an application for coverage and to further improve the application processing time for the underwriter.
6. On June 25th, July 23rd and July 26th, Aon Benfield received for dissemination to the reinsurers’ notice of four (4) “new” large loss serious injury claims.
7. On June 26th, staff met with underwriting representatives from the Travelers at its Orlando service office to discuss common issues relevant to the effective management of the FWCJUA book of business.
8. On June 27th, staff conducted the first of two reviews of serious injury claims and claims operations in Orlando at Travelers’ service office.
9. On June 28th, the FWCJUA/Travelers referred one (1) account for suspected premium fraud and one (1) serious injury case for suspected claimant fraud to Travelers SIU for investigation.
10. As of June 30th, the current cumulative uncollectible premium was 14.33%, which is slightly better than the established 2012 target of 14.35%.
11. On July 10th & August 8th, prior month-end reports were submitted to DFS, Division of Workers Compensation, Bureau of Compliance identifying the names and addresses of employers whose policies have either cancelled or non-renewed and the names and addresses of applicants who have applied but did not purchase FWCJUA coverage.
12. On July 16th, staff conducted an additional review of thirteen (13) serious injury claims with the Travelers serious injury adjuster that was unable to attend the FWCJUA’s Semi-Annual Claims review conducted on June 27th.
13. On July 16th, the FWCJUA’s website was amended to add information and a link regarding the Reemployment Services Program provided for in Section 440.491, Florida Statutes.
14. On July 18th, the Operations Manager reviewed the underwriting department process and discovered possible opportunities to enhance and improve the processing time for the Underwriter.
15. On July 20th, staff received Travelers’ 2012 Second Quarter Self Audit Performance Report, resulting in a cumulative score of 99%.
16. On July 23rd, the FWCJUA filed reinsurance recoveries with Aon Benfield on seven (7) of the FWCJUA’s serious injuries, whose total paid amounts exceeded the reinsurance limits within the accident years.
17. On July 25th, staff responded to Milliman’s request for data and other information evaluated as of June 30, 2012 in order to determine whether to effectuate a premium level change effective January 1, 2013.
19. On July 31st, the FWCJUA distributed 3,901 dividend checks totaling $12,045,380.85 to eligible Tier 1, 2 and 3 policyholders with policy effective dates of 7/1/2004 through 12/31/2005.
20. On August 6th, replaced Bookkeeper/Clerk who departed August 1st.
21. On August 8th, the 2012 Second Quarter Financial Statement was filed in which the FWCJUA recognized a $63,104,929 surplus, with a Subplan D deficit of $681,744.
22. On August 10th, the third quarter review of the book of business identified three (3) accounts exceeding $300K EAP and staff determined that circumstances were substantially insufficient to initiate implementation of the FWCJUA Loss Sensitive Rating Plan (LSRP); thus, given the FWCJUA currently only has three (3) accounts at such a premium level, there remains insufficient activity to warrant activating the Plan.
24. On August 21st, the FWCJUA reported statistical data required of 626.9891(6), Florida Statutes, to the Division of Insurance Fraud it experienced implementing and maintaining an anti-fraud plan.
### FWCJUA, INC.
SUMMARY OF POLICYHOLDER RETURN PREMIUM DIVIDENDS
AS OF 07/31/2012

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TIER 1, 2, &amp; 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount</td>
<td>$26,602,018</td>
<td>$12,178,029</td>
<td>$5,149,549</td>
<td>$5,669,727</td>
<td>$2,746,322</td>
<td>$858,391</td>
</tr>
<tr>
<td># Policies</td>
<td>7,279</td>
<td>4,661</td>
<td>762</td>
<td>1,257</td>
<td>770</td>
<td>453</td>
</tr>
<tr>
<td>Adjustments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checks issued</td>
<td>Amount</td>
<td>$26,186,045</td>
<td>$12,048,645</td>
<td>$4,993,499</td>
<td>$5,609,254</td>
<td>$2,693,522</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td># Checks</td>
<td>7,153</td>
<td>3,942</td>
<td>755</td>
<td>1,250</td>
<td>759</td>
</tr>
<tr>
<td>Outstanding as of 07/31/12</td>
<td>$529,310</td>
<td>$12,048,645</td>
<td>$198,909</td>
<td>$202,234</td>
<td>$120,143</td>
<td>$8,023</td>
</tr>
<tr>
<td></td>
<td># Checks</td>
<td>185</td>
<td>3,942</td>
<td>54</td>
<td>81</td>
<td>34</td>
</tr>
<tr>
<td>Outstanding $$ as % of Amount Issued</td>
<td>2.0%</td>
<td>100.0%</td>
<td>4.0%</td>
<td>3.6%</td>
<td>4.5%</td>
<td>1.0%</td>
</tr>
</tbody>
</table>

### POLICYHOLDER RETURN OF PREMIUM DIVIDEND RESULTS
(As of July 31, 2012)
Net Dividend for All Years: $26,197,083

<table>
<thead>
<tr>
<th>RETURN OF PREMIUM DIVIDEND DETAILS</th>
<th>PY 2004-2005 TIER 1, TIER 2, TIER 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISPOSITION OF CHECKS ISSUED</td>
<td># OF RECIPIENTS</td>
</tr>
<tr>
<td>Cashed *</td>
<td>0</td>
</tr>
<tr>
<td>Outstanding</td>
<td>3942</td>
</tr>
<tr>
<td>CHECKS - SUBTOTAL</td>
<td>3942</td>
</tr>
</tbody>
</table>

| DISPOSITION OF OTHER PAYABLE DOLLARS | # OF IMPACTED | PAYABLE DOLLARS RETAINED | % OF TOTAL PAYABLE DOLLARS |
| Paid Outstanding Collection Fees   | 23 | $20,566 | 0.2% |
| Paid Outstanding Premium           | 38 | $68,928 | 0.6% |
| Withheld for Noncompliance with Final Audit in another Policy Year. (Possible Forfeiture) | 34 | $39,890 | 0.3% |
| OTHER - SUBTOTAL                   | 95 | $129,384 | 1.1% |

TOTAL BOARD DECLARED 06/13/2012 4,037 $12,178,029