U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT HIGHMARK BLUE CROSS BLUE SHIELD

Report Number 1A-10-13-16-020
November 10, 2016

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Highmark Blue Cross Blue Shield

Report No 1A-10-13-16-020 **November 10, 2016**

Background
Highmark Blue Cross Blue Shield (Highmark) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

Why Did We Conduct the Audit?
The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Highmark's information technology (IT) environment.

What Did We Audit?
The scope of this audit centered on the information systems used by Highmark to process and store data related to insurance claims for FEHBP members.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?
Our audit of the IT security controls at Highmark determined that:

- Highmark has established an IT security management program. However, we noted the following areas of concern in the program:
  - Highmark does not have a formal training requirement for individuals with specialized IT security responsibility.
  - Highmark is not in compliance with its corporate policy to update IT security policies on a routine basis.
- Highmark has implemented a variety of controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, we noted several areas of concern related to Highmark's access controls:
  - Physical controls surrounding Highmark's secondary data center could be improved.
  - Highmark does not routinely audit physical access badges.
  - There is no routine audit of all user accounts.
  - Multi-factor authentication is not required to gain privileged access to Highmark information systems.
- Highmark has implemented an adequate incident response and network security program.
- Highmark has developed formal configuration management policies. However, we noted several areas of concern related to Highmark's configuration management program:
  - Baseline security configuration standards have not been developed for all operating platforms used by Highmark.
  - There is no routine audit to ensure that current configuration settings are in compliance with security configuration standards.
  - Our vulnerability scan results indicated that Highmark servers contained unsupported software and were missing security patches on multiple applications.
- Highmark's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications.
- Highmark has implemented many controls in its claims adjudication processes to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

the Act	**The Federal Employees Health Benefits Act**
Association	**Blue Cross Blue Shield Association**
BCBS	**Blue Cross and Blue Shield**
CFR	**Code of Federal Regulations**
DISA STIG	**Defense Information Systems Agency Standard Technical Implementation Guide**
FEHBP	**Federal Employees Health Benefit Plan**
FISCAM	**Federal Information Systems Control Audit Manual**
GAO	**U.S. Government Accountability Office**
Highmark	**Highmark BlueCross BlueShield**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology's Special Publication**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**

TABLE OF CONTENTS

I. BACKGROUND

This final report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) claims by Highmark Blue Cross Blue Shield (Highmark).

The audit was conducted pursuant to FEHBP contract CS 1039; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The FEHBP was established by the Federal Employees Health Benefits Act (the Act), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

The Blue Cross Blue Shield Association (Association), on behalf of participating Blue Cross and Blue Shield (BCBS) plans, has entered into a Government-wide Service Benefit Plan contract (CS 1039) with OPM to provide a health benefit plan authorized by the FEHB Act. The Association delegates authority to participating local BCBS Plans throughout the United States, such as Highmark, to process the health benefit claims of its federal subscribers.

The Association has established a Federal Employee Program Director's Office in Washington, D.C. to provide centralized management for the Service Benefit Plan. The Federal Employee Program Director's Office coordinates the administration of the contract with the Association, member BCBS Plans, and OPM.

All Highmark personnel that worked with the auditors were helpful and open to ideas and suggestions. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

This was our first audit of Highmark's information technology (IT) general and application controls. We discussed the results of our audit with OPM and Highmark representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Highmark's information technology (IT) environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to Highmark's claims processing systems.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of Highmark's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of Highmark's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by Highmark to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication process. The business processes reviewed are primarily located in Highmark's Camp Hill and Pittsburgh, Pennsylvania facilities. This was our first audit of Highmark's information technology general and application controls.

The on-site portion of this audit was performed in January and February of 2016. We completed additional audit work before and after the on-site visit at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at Highmark as of March 2016.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Highmark. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps but we determined that it was adequate to achieve our audit objectives.

However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.
In conducting this review we:

- Gathered documentation and conducted interviews;
- Reviewed Highmark's business structure and environment;
- Performed a risk assessment of Highmark's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM); and
- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating Highmark's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;
- U.S. Office of Management and Budget (OMB) Circular A-130, Appendix III;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- COBIT 5: A Business Framework for Governance and Management of Enterprise IT
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, An Introduction to Computer Security: The NIST Handbook;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether Highmark's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Highmark was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Management

Security management controls encompass the policies and procedures that are the foundation of an organization's overall IT security program. We examined Highmark's ability to develop and review security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various systems-related controls. We also examined personnel policies related to hiring, training, and terminating employees.

We found that Highmark has implemented a series of formal policies and procedures that comprise its IT security program. Specifically, we noted that Highmark:

- Has documented policies and procedures for IT management;
- Maintains an adequate risk management methodology that includes regular risk assessments across multiple functional areas; and
- Has procedures to verify that employees are vetted for their position.

The following sections document opportunities for improvement related to Highmark's security management controls.

1) Specialized Training for IT Professionals

Highmark requires annual privacy and security training for all employees. However, Highmark does not have a formal training requirement for individuals with specialized IT security responsibility.

NIST SP 800-53, Revision 4, explains that IT staff should receive "adequate security-related technical training specifically tailored for their assigned duties."

Requiring employees with specialized IT security responsibility to take routine training relevant to their assigned duties increases their ability to address the constant changes in IT security best-practices.

Recommendation 1

We recommend that Highmark require routine job-related training for employees with specialized IT security responsibility.

Plan Response:

"The Plan agrees with the recommendation. The Plan is implementing a training plan that provides opportunities for specialized training for individuals who work in specialized IT areas, such as GIAC, DWASP, CRISC, OSCP, ENCE, CISSP, and Security+ training and certification opportunities for a myriad of employees in IT Security. This training plan will remain in place each year and will be updated prospectively with additional specialized IT trainings as they are identified, including the requirement for employees in specialized IT areas to complete a specific training regimen by 2nd quarter 2016."

OIG Comment:

As part of the audit resolution process, we recommend that Highmark provide OPM's Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this report that Highmark agrees to implement.

2) **Annual Policy Review**

Highmark maintains a corporate policy that requires the overall IT security program be reviewed annually. However, this policy does not require each individual security policy be reviewed, and we identified several policies that had not been reviewed or updated in more than two years.

Several IT policies had not been reviewed or updated in more than two years.

FISCAM states that policies "should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in . . . mission or the types and configuration of computer resources in use."

Failure to routinely review and/or update IT policies increases the possibility that current security risks will not be appropriately addressed.

Recommendation 2

We recommend that Highmark adjust its corporate security policy to require the annual review and/or update of all IT policies.

Plan Response:

"The Plan agrees with the recommendation. The Plan is currently in the process of implementing a new Governance, Risk, and Compliance (eGRC) solution that will address

this recommendation by 3rd quarter 2016. Policy owners will be assigned and required to review policies annually. Documented evidence of review and approval will be maintained within the eGRC solution for future reference."

B. Access Controls

Access controls are the policies, procedures, and tools used to prevent or detect unauthorized physical or logical access to sensitive resources. We examined the physical access controls at Highmark's facilities and data centers located in [redacted], Pennsylvania. We also examined the logical access controls protecting sensitive data in Highmark's network environment and applications.

The access controls observed during this audit include, but are not limited to:

- Procedures to appropriately grant and adjust logical access to applications and software resources;
- Robust physical and environmental controls within the primary data center; and
- Role-based access provisioning program with documented non-compatible roles.

The following sections document opportunities for improvement related to Highmark's physical and logical access controls.

1) Physical Access Controls at Secondary Data Center

Highmark maintains a secondary/backup data center used for load balancing and backup of its virtual desktop infrastructure functionality. Access to this facility is controlled by an electronic badge reader. However, we expect data centers of all FEHBP contractors to also have the following additional controls that were not present at this Highmark facility:

- [redacted]
- [redacted]
- [redacted]

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data. Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

Recommendation 3

We recommend that Highmark implement [redacted] at its secondary data center.

Plan Response:

"The Plan agrees with the recommendation. The Plan has a project that is currently underway to address all elements of this recommendation by 4th quarter 2016."

2) Physical Access Provisioning

Physical access to Highmark facilities is controlled through an electronic badge access system. Highmark's procedure is to assign each employee a unique electronic badge, and the system is designed to log when each individual uses their badge to enter the facility. However, we found a large number of instances where it appeared that Highmark may have allocated multiple badges to one individual, but Highmark was unable to determine whether these were duplicate badges assigned to a single individual, or if they were unique badges assigned to multiple individuals with the same name. This confusion is the result of Highmark's badging system not using a unique identifier for each individual, and only referencing them by first and last name. As a result, Highmark is not able to fully leverage the system's logging capabilities to determine which specific individuals enter and exit its facilities. Additionally, Highmark is exposed to increased risk that an individual may be granted or maintain an inappropriate level of access.

Highmark also uses the badge system to limit access to specific physical areas that are considered secure. On a quarterly basis, Highmark corporate security sends lists of all users with access to each secure area to that area's "gate keeper" so that the gate keeper can audit the list for appropriateness. However, there is no requirement for a formal response from the gate keeper, nor is there an escalation process to ensure that an adequate review was performed. In addition, this review is only performed for the secure areas, and not for general access to Highmark facilities.

Finally, our test work found a number of instances where individuals' access badges remained active past their termination date. This applied to both secure areas subject to the current quarterly review and general Highmark facility access.

Our test work found a number of instances where individuals' access badges remained active past their termination date.

NIST SP 800-53, Revision 4, necessitates that an organization must enforce physical access authorization by verifying individual access authorizations and maintaining physical access audit logs.

FISCAM requires that "Management regularly reviews the list of persons with physical access to sensitive facilities." NIST SP 800-53, Revision 4, expounds on this requirement and states that the organization "Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; … Reviews the access list detailing authorized facility access by individuals; and … Removes individuals from the facility access list when access is no longer required."

Failure to maintain adequate controls over physical access badges increases the risk that individuals could gain unauthorized entry to Highmark facilities and access sensitive or proprietary information.

Recommendation 4

We recommend that Highmark implement a process to routinely review all active physical access badges. This review should ensure that only one badge is assigned to every individual authorized to enter its facilities unescorted; that access was removed promptly upon an individual's termination or transfer; and that the level of access assigned to each individual is appropriate. This process should also require that the results of each review be maintained for audit purposes.

Plan Response:

"The Plan agrees with the recommendation. The Plan completed a review of all assigned access badges in 2nd quarter 2016 and validated that physical access to facilities was restricted to authorized personnel. The Plan is currently implementing a new Human Capital Management system that will address this recommendation by 4th quarter 2016. In addition, a process to review all active physical access badges to the plan's facilities will be performed on a quarterly basis beginning in 4th quarter 2016. The review will ensure that only one badge is assigned to every individual authorized to enter the facility, that access is removed promptly upon termination/transfer, and that access levels remain appropriate."

3) Logical Access

Logical access to Highmark systems is generally controlled by a single unique user ID and password assigned to each user. However, we found several instances where Highmark had

allocated multiple user accounts to individuals without a valid business justification – a practice that is not compliant with Highmark's policy.

Our test work also detected numerous instances where an individual's user accounts remained active beyond the period of employment (this included both employees and contractors).

Finally, although Highmark stated that it had a procedure in place to routinely audit logical access, it was unable to produce any evidence to support that such reviews actually occurred.

As a result of these issues with logical access controls, Highmark is exposed to increased risk that authorized individuals may have an inappropriate level of information system access, or that an adversary could gain unauthorized access to sensitive data.

FISCAM requires that the organization match personnel files to actual system user accounts to ensure that all terminated or transferred employees are removed from the system. In addition, NIST SP 800-53, Revision 4, requires "The organization [to review] . . . the privileges assigned to [users] to validate the need for such privileges; and … Reassigns or removes privileges . . . to correctly reflect organizational mission/business needs."

Recommendation 5

We recommend that Highmark implement a process to routinely audit all user accounts. This audit should ensure that only one user ID is assigned to every employee and vendor authorized to access Highmark systems, that user accounts are disabled promptly upon an individual's termination; and that the level of access assigned to each individual is appropriate.

Plan Response:

"The Plan disagrees with the observation that there is not a process in place to routinely audit user accounts. The Plan currently reviews user access privileges annually in alignment with Model Audit Rule (MAR) compliance requirements. The Plan will make enhancement[s] to perform a quarterly review of user accounts in alignment with SOC2 compliance standards by 4th quarter 2016."

OIG Comment:

Highmark stated that it had a procedure in place to routinely audit logical access, but as stated above, the Plan has not produced any evidence to indicate that such reviews have

occurred. Even if an audit process were in place, the anomalies detected by our test work indicate that this process is not fully effective. As part of the audit resolution process, we recommend that Highmark provide OPM's HIO with evidence that it has implemented a routine audit process for all user accounts that encompasses the control enhancement referenced in the Plan's response.

4) Privileged User Authentication

All Highmark information systems, at both the administrator and user level, can be accessed via single-factor authentication (i.e., a password). The use of multi-factor authentication (e.g., a password and a dynamic pin) would increase the security of all user accounts, but at a minimum should be immediately implemented for privileged user (administrator) accounts.

NIST SP 800-53, Revision 4, necessitates that "The information system implements multifactor authentication for network access to privileged accounts." Failure to require multifactor authentication on privileged accounts increases the risk of unauthorized access to sensitive data and the ability to modify system controls.

Recommendation 6

We recommend that Highmark implement multi-factor authentication for privileged user accounts on its information systems.

Plan Response:

"The Plan agrees with the recommendation. The Plan is currently in the process of implementing a [redacted] "Privileged Account Security" solution that will enforce multi-factor authentication and ongoing monitoring for privileged accounts by 4th quarter 2016."

C. Network Security

Network security includes the policies and controls in place to manage and monitor the use and security of a computer network and network-accessible resources.

We noted that Highmark has implemented the following network security controls:

- A documented incident response methodology;
- Intrusion detection and prevention systems; and
- Thorough network segmentation.

Highmark has a variety of controls in place to monitor and manage network traffic.

Nothing came to our attention to indicate that Highmark has not implemented adequate controls regarding network security.

D. Configuration Management

Configuration management controls are the policies and procedures that ensure that system software such as operating systems and databases are configured securely. We evaluated Highmark's configuration management program as it relates to the systems that support the processing of FEHBP claims, and determined that the following controls were in place:

- Configuration management policies based on the Defense Information Systems Agency Standard Technical Implementation Guide (DISA STIG);
- Established baseline configurations; and
- A system software change control process.

The following sections document opportunities for improvement related to Highmark's configuration management controls.

1) Baseline Configurations

Highmark utilizes the DISA STIG as a guideline for the configuration of its servers. Using this guidance, Highmark has developed detailed baseline configuration standards custom to its environment for its [redacted] servers, but has not developed this detailed documentation for its [redacted] environments.

NIST SP 800-53, Revision 4, requires that "The organization develops, documents, and maintains under configuration control, a current baseline of the information system."

Failure to document detailed baseline configurations increases the risk that servers with insecure configuration settings exist in the organization's technical environment.

Recommendation 7

We recommend that Highmark document detailed secure configuration baselines for all operating platforms used in its technical environment.

Plan Response:

"The Plan agrees with the recommendation. The Plan will expand to include configuration baselines for all operating platforms used in its technical environment by 4th quarter 2016."

2) Configuration Compliance Auditing

Highmark routinely audits the current/actual settings of its [redacted] servers against the approved baseline configuration for compliance. However, as mentioned above, Highmark does not have an approved baseline for [redacted], and therefore there are no approved settings against which to audit.

FISCAM states that organizations should require, "Current configuration information [to be] routinely monitored for accuracy. Monitoring should address the baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected.

Recommendation 8

We recommend that Highmark conduct routine configuration compliance audits on [redacted] platforms to ensure they are in compliance with the approved baselines.

Plan Response:

"The Plan agrees with the recommendation. The Plan will expand the routine DISA-STIG compliance scans against the [redacted] environments to confirm that hardening measures are taken in accordance with the latest DISA-STIG standards by 4th quarter 2016. In the event that the appropriate level of detail is not available and/or the baseline configuration cannot be met, additional documentation will be updated through a Maintenance Service Request (MSR) ticket."

3) Vulnerability Scan Results

Highmark has implemented a process to routinely scan its information systems for known vulnerabilities using an automated scanning tool. However, when we compared the results of Highmark's vulnerability scans to the results of scans that we ran independently as part of this audit, it appeared that the tools being used by Highmark failed to identify several known weaknesses. The specific vulnerabilities that we identified will not be detailed in this report, but are summarized at a high level below. Copies of the full scan reports were provided directly to Highmark during the audit.

Unsupported Software

Our scans detected the presence of software that is no longer supported by the vendors, and have known security vulnerabilities. This included third-party applications and also one operating system. Highmark did provide evidence indicating that it was previously aware of some of this unsupported software, and that a short term remediation plan was in place. However, Highmark did not have a defined plan to remove or upgrade the majority of the unsupported software we detected.

FISCAM states that "Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms."

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 9

We recommend that Highmark remove the unsupported software detected during this audit from its environment.

Plan Response:

"The Plan agrees with the recommendation. The Plan will perform a formally documented risk mitigation treatment(s) through the use of a Maintenance Service Request (MSR) ticket to maintain supporting documentation where unsupported software cannot be removed or will remove unsupported software identified during this audit by 3rd quarter 2016."

Recommendation 10

We recommend that Highmark implement a formal software lifecycle management methodology to ensure that only current and supported versions of system software are installed on the production servers.

Plan Response:

"The Plan agrees with the recommendation. The Plan is currently updating our software lifecycle management methodology to address gaps in ongoing monitoring of installed software components and expects to complete this activity by 2nd quarter 2016."

Application Patching

Highmark has implemented a standard patch management process for all operating systems. Our scans determined that Highmark's operating system patches were generally up to date.

However, our scans also detected that third-party applications were not always patched in a timely manner (missing patches that are over 60 days old). This included several instances where specific patches were missing on a widespread basis throughout the network, and also instances of individual servers that were missing a large number of patches. Highmark acknowledged these missing patches and cited anomalies in the patching process as a reason why the patches are missing. Highmark indicated the applications will be resolved within the next 30 days.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53, Revision 4, requires that "The organization … identifies, reports, and corrects information system flaws; … and installs security-relevant software and firmware updates" promptly.

The vulnerabilities identified in our test work increase the risk that a malicious attack on Highmark's technical environment would be successful.

Recommendation 11

We recommend that Highmark address the specific patches missing from third party applications that were detected in our vulnerability scans.

Plan Response:

"The Plan agrees with the recommendation. The Plan will perform a formally documented risk mitigation treatment(s) through the use of a Maintenance Service Request (MSR) ticket or apply requisite patches identified during this audit by 2nd quarter 2016."

Recommendation 12

We recommend that Highmark perform an analysis to determine the root cause of the third party patching anomalies. This should include analysis of both the patches missing on a widespread basis and the individual applications that were missing a large number of patches, as the root cause for each issue may be unique. Based on this analysis, Highmark should also

update its procedures and/or implement additional controls to address the problem of missing patches in its environment.

Plan Response:

"The Plan agrees with the recommendation. The Plan's patch management standard includes performing regularly scheduled periodic maintenance. All assets will be scheduled for periodic maintenance at least twice a year. This maintenance window will be used to apply the current vendor recommended maintenance level. The Plan will enhance the current patch management process to formally document an exception and assist the application owner(s) with resolution where application or hardware dependencies prevent application of the current maintenance levels by 3rd quarter 2016."

E. Contingency Planning

We reviewed elements of Highmark's contingency planning program to determine whether controls were in place to prevent or minimize interruptions to business operations when disrupting events occur. Our review indicated that Highmark has developed the following plans and procedures:

- Disaster recovery plan;
- Business continuity plan; and
- Emergency response procedures.

Highmark maintains plans to ensure continuity of operations in the event of disasters.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1. Highmark has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that Highmark has not implemented adequate controls regarding contingency planning.

F. Claims Adjudication

The following sections detail our review of the applications and business processes supporting Highmark's claims adjudication process. Highmark prices and adjudicates claims through its local claims processing system and then through the Association's FEP Direct nationwide claims adjudication system. Our review included the following processes: application change control, claims lifecycle, and provider debarment.

1) **Application Configuration Management**

We evaluated the policies and procedures governing application development and change control of Highmark's claims processing systems.

Highmark has implemented policies and procedures related to application configuration management, and has also adopted a system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approvals of software modifications:

- Policies and procedures that allow modifications to be tracked throughout the change process;
- Code, unit, system, and quality testing are conducted in accordance with industry standards; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

Nothing came to our attention to indicate that Highmark has not implemented adequate controls related to the application configuration management process.

2) **Claims Input, Processing, and Output Controls**

We evaluated the input, processing, and output controls associated with Highmark's claims adjudication process. We have determined the following controls are in place over Highmark's claims adjudication system:

- Sufficient controls over the input and processing of claims;
- Documented policies and procedures for full reconciliation of claim output files; and
- Quality assurance reviews of each step in the lifecycle of a claim.

Nothing came to our attention to indicate that Highmark has not implemented adequate controls related to the claims process.

3) **Debarment**

We evaluated Highmark's procedures for updating its claims system with debarred provider information. Highmark downloads the OPM OIG debarment list every month, provider flags are placed in the claims processing system, and a quality assurance validation is conducted. Any claim submitted by a debarred provider is flagged by Highmark to adjudicate through the OPM OIG debarment process to include initial notification, a 15-day grace period, and then denial of claims.

Nothing came to our attention to indicate that Highmark has not implemented adequate controls related to debarment.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

INFORMATION SYSTEMS AUDIT GROUP

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], Senior Team Leader

[redacted], Group Chief

APPENDIX

BlueCross BlueShield Association

An Association of Independent Blue Cross and Blue Shield Plans

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

June 17, 2016

[redacted], Group Chief
Claims & IT Audits Group,
U.S. Office of Personnel Management
1900 E Street, Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT AUDIT REPORT
Highmark Blue Cross Blue Shield IT Audit
Plan Codes 363
Audit Report Number 1A-10-13-16-020
(Dated April 12, 2016)

The following represents the Plan's response as it relates to the recommendations included in the draft report.

A. Security Management

1. Specialized Training for IT Professionals

Recommendation 1

We recommend that Highmark require routine job-related training for employees with specialized IT security responsibility.

Plan Response

The Plan agrees with the recommendation. The Plan is implementing a training plan that provides opportunities for specialized training for individuals who work in specialized IT areas, such as GIAC, DWASP, CRISC, OSCP, ENCE, CISSP, and Security+ training and certification opportunities for a myriad of employees in IT Security. This training plan will remain in place each year and will be updated prospectively with additional specialized IT trainings as they are identified, including the requirement for employees in specialized IT areas to complete a specific training regimen by 2nd quarter 2016.

2. Annual Policy Review

Recommendation 2

We recommend that Highmark adjust its corporate security policy to require the annual review and/or update of all IT policies.

Plan Response

The Plan agrees with the recommendation. The Plan is currently in the process of implementing a new Governance, Risk, and Compliance (eGRC) solution that will address this recommendation by 3rd quarter 2016. Policy owners will be assigned and required to review policies annually. Documented evidence of review and approval will be maintained within the eGRC solution for future reference.

B. Access Controls

1. Physical Access Controls at Secondary Data Center

Recommendation 3

We recommend that Highmark implement piggybacking prevention controls, multi-factor authentication, and video surveillance at its secondary data center.

Plan Response

The Plan agrees with the recommendation. The Plan has a project that is currently underway to address all elements of this recommendation by 4th quarter 2016.

2. Physical Access Provisioning

Recommendation 4

We recommend that Highmark implement a process to routinely review all active physical access badges. This review should ensure that only one badge is assigned to every individual authorized to enter its facilities unescorted; that access was removed promptly upon an individual's termination or transfer; and that the level of access assigned to each individual is appropriate. This process should also require that the results of each review be maintained for audit purposes.

Plan Response

The Plan agrees with the recommendation. The Plan completed a review of all assigned access badges in 2nd quarter 2016 and validated that physical access to facilities was restricted to authorized personnel. The Plan is currently implementing a new Human Capital Management system that will address this recommendation by 4th quarter 2016. In addition, a process to review all active physical access badges to the plan's facilities will be performed on a quarterly basis beginning in 4th quarter 2016. The review will ensure that only one badge is assigned to every individual

authorized to enter the facility, that access is removed promptly upon termination/transfer, and that access levels remain appropriate.

3. Logical Access

Recommendation 5

We recommend that Highmark implement a process to routinely audit all user accounts. This audit should ensure that only one user ID is assigned to every employee and vendor authorized to access Highmark systems, that user accounts are is disabled promptly upon an individual's termination; and that the level of access assigned to each individual is appropriate.

Plan Response

The Plan disagrees with the observation that there is not a process in place to routinely audit user accounts. The Plan currently reviews user access privileges annually in alignment with Model Audit Rule (MAR) compliance requirements. The Plan will make enhancement to perform a quarterly review of user accounts in alignment with SOC2 compliance standards by 4th quarter 2016. See **Attachment A**.

4. Privileged User Authentication

Recommendation 6

We recommend that Highmark implement multi-factor authentication for privileged user accounts on its information systems.

Plan Response

The Plan agrees with the recommendation. The Plan is currently in the process of implementing a [redacted] "Privileged Account Security" solution that will enforce multi-factor authentication and ongoing monitoring for privileged accounts by 4th quarter 2016.

C. Network Security

No recommendations were noted.

D. Configuration Management

1. Baseline Configurations

Recommendation 7

We recommend that Highmark document detailed secure configuration baselines for all operating platforms used in its technical environment.

Plan Response

The Plan agrees with the recommendation. The Plan will expand to include

configuration baselines for all operating platforms used in its technical environment by 4th quarter 2016.

2. Configuration Compliance Auditing

Recommendation 8

We recommend that Highmark conduct routine configuration compliance audits on [redacted] platforms to ensure they are in compliance with the approved baselines.

Plan Response Plan Response

The Plan agrees with the recommendation. The Plan will expand the routine DISA-STIG compliance scans against the [redacted] environments to confirm that hardening measures are taken in accordance with the latest DISA-STIG standards by 4th quarter 2016. In the event that the appropriate level of detail is not available and/or the baseline configuration cannot be met, additional documentation will be updated through a Maintenance Service Request (MSR) ticket.

3. Vulnerability Scan Results

Recommendation 9

We recommend that Highmark remove the unsupported software detected during this audit from its environment.

Plan Response Plan Response

The Plan agrees with the recommendation. The Plan will perform a formally documented risk mitigation treatment(s) through the use of a Maintenance Service Request (MSR) ticket to maintain supporting documentation where unsupported software cannot be removed or will remove unsupported software identified during this audit by 3rd quarter 2016.

Recommendation 10

We recommend that Highmark implement a formal software lifecycle management methodology to ensure that only current and supported versions of system software are installed on the production servers.

Plan Response Plan Response

The Plan agrees with the recommendation. The Plan is currently updating our software lifecycle management methodology to address gaps in ongoing monitoring of installed software components and expects to complete this activity by 2nd quarter 2016.

Recommendation 11

We recommend that Highmark address the specific patches missing from

third party applications that were detected in our vulnerability scans.

Plan Response Plan Response
The Plan agrees with the recommendation. The Plan will perform a formally documented risk mitigation treatment(s) through the use of a Maintenance Service Request (MSR) ticket or apply requisite patches identified during this audit by 2nd quarter 2016.

Recommendation 12
We recommend that Highmark perform an analysis to determine the root cause the third party patching anomalies. This should include analysis of both the patches missing on a widespread basis and the individual applications that were missing a large number of patches, as the root cause for each issue may be unique. Based on this analysis, Highmark should also update its procedures and/or implement additional controls to address the problem of missing patches in its environment.

Plan Response Plan Response
The Plan agrees with the recommendation. The Plan's patch management standard includes performing regularly scheduled periodic maintenance. All assets will be scheduled for periodic maintenance at least twice a year. This maintenance window will be used to apply the current vendor recommended maintenance level. The Plan will enhance the current patch management process to formally document an exception and assist the application owner(s) with resolution where application or hardware dependencies prevent application of the current maintenance levels by 3rd quarter 2016.

E. Contingency Planning

******Redacted by OPM OIG – not relevant to final audit report******

We appreciate the opportunity to provide our response to each of the recommendations in this report and request that our comments be included in their entirety and are made a part of the Final Audit Report. If you have any questions, please contact me at [redacted] or [redacted].

Sincerely,

[redacted], CISA
Managing Director, FEP Program Assurance

cc: [redacted], Highmark
[redacted], OPM
[redacted], FEP
[redacted], FEP
[redacted], FEP

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100

-- CAUTION --