



## **Consumer Financial Protection Bureau (CFPB)**

Contract #: GS-10F-0062R  
Task Order #: CFP-12-K-00011

### **Independent Performance Audit of CFPB Operations and Budget**

**Submitted November 13, 2012 by:**

ASR Analytics, LLC  
1389 Canterbury Way  
Potomac, MD 20854

Federal TIN: 20-1204680  
DUNS: 15-108-3305  
[www.asranalytics.com](http://www.asranalytics.com)

**Submitted to:**

Consumer Financial Protection Bureau  
Ms. Alicia McDonald ([alicia.mcdonald@cfpb.gov](mailto:alicia.mcdonald@cfpb.gov))  
1700 G Street, NW  
Washington, DC 20552





November 13, 2012

Mr. Richard Cordray  
Director  
Consumer Financial Protection Bureau  
1700 G Street NW  
Washington, DC 20552

Dear Mr. Cordray:

On behalf of ASR Analytics, LLC (ASR), I am pleased to enclose the attached report, which presents the results of our independent performance audit of the Consumer Financial Protection Bureau (CFPB). This audit was commissioned by the CFPB in accordance with the Full-Year Continuing Appropriations Act, 2011 (Pub. L. 112-10) of April 15, 2011, Title V, Section 1573 (a), which amended the Dodd-Frank Wall Street Reform and Consumer Protection Act to require an annual independent audit of the operations and budget of the bureau (12 USC 5496a). ASR performed this work between July 6, 2012 and November 13, 2012.

For this fiscal year 2012 performance audit, ASR reviewed three key areas of operations identified by the Bureau: (1) Privacy Programs, Policies and Processes; (2) Travel Systems and Services, including the travel card program; and (3) the CFPB Budget. In addition, the CFPB requested an evaluation of corrective actions that it has taken to address findings and recommendations from the fiscal year 2011 performance audit—which focused on five areas of performance: (1) Communications and Transparency; (2) Consumer Response; (3) Human Capital and Organizational Development; (4) Information Technology; and (5) the CFPB Budget.

To evaluate the CFPB's operations and performance across these areas, we relied on a combination of physical, documentary, and testimonial evidence, most of which was provided by the CFPB. We reviewed more than 700 artifacts, including policy and planning documents, status reports, briefing memos, meeting minutes, discussion decks, statements of work, and other sources. In addition, we held more than 100 meetings with CFPB personnel and other stakeholders.

A draft of this report was shared with all participating stakeholders at the CFPB for review and comment. CFPB staff provided us with oral and written comments on the draft report, including several technical clarifications and suggestions, which we incorporated where appropriate. Key contributors to this report included Edward Hau, Michele Lebar, Shal Malhotra, Bob Siegel, Michael Stavrianos, and Melissa Toledo.

Sincerely,

A handwritten signature in blue ink that reads "Michael Stavrianos". The signature is fluid and cursive, with a long horizontal line extending from the end of the name.

Michael Stavrianos  
Founding Principal  
ASR Analytics, LLC

cc: Mr. Victor Prince, Chief Operating Officer, Consumer Financial Protection Bureau

# Table of Contents

|                    |  |            |
|--------------------|--|------------|
| <b>Section 1:</b>  | <b>Executive Summary .....</b>                           | <b>1</b>   |
| 1.1                | Background.....  | 1          |
| 1.2                | Compliance with Government Auditing Standards.....       | 1          |
| 1.3                | Organization of this Report.....                         | 2          |
| 1.4                | Summary of Findings and Recommendations .....            | 4          |
| <b>Section 2:</b>  | <b>Privacy.....</b>                                      | <b>5</b>   |
| 2.1                | Scope of Audit .....                                     | 5          |
| 2.2                | Evaluation Criteria.....                                 | 6          |
| 2.3                | Findings and Recommendations.....                        | 9          |
| <b>Section 3:</b>  | <b>Travel Policy.....</b>                                | <b>56</b>  |
| 3.1                | Scope of Audit .....                                     | 56         |
| 3.2                | Evaluation Criteria.....                                 | 56         |
| 3.3                | Findings and Recommendations.....                        | 59         |
| <b>Section 4:</b>  | <b>Budget .....</b>                                      | <b>67</b>  |
| 4.1                | Scope of Audit .....                                     | 67         |
| 4.2                | Evaluation Criteria.....                                 | 69         |
| 4.3                | Findings and Recommendations (FY12 Audit).....           | 71         |
| 4.4                | Findings and Recommendations (FY11 Audit).....           | 85         |
| <b>Section 5:</b>  | <b>Communications and Transparency .....</b>             | <b>88</b>  |
| 5.1                | Scope of Audit .....                                     | 88         |
| 5.2                | Findings and Recommendations.....                        | 88         |
| <b>Section 6:</b>  | <b>Consumer Response.....</b>                            | <b>106</b> |
| 6.1                | Scope of Audit .....                                     | 106        |
| 6.2                | Findings and Recommendations.....                        | 108        |
| <b>Section 7:</b>  | <b>Human Capital and Organizational Development.....</b> | <b>123</b> |
| 7.1                | Scope of Audit .....                                     | 123        |
| 7.2                | Findings and Recommendations.....                        | 123        |
| <b>Section 8:</b>  | <b>Information Technology .....</b>                      | <b>135</b> |
| 8.1                | Scope of Audit .....                                     | 135        |
| 8.2                | Findings and Recommendations.....                        | 135        |
| <b>Appendix A:</b> | <b>List of CFPB Officials who Provided Input .....</b>   | <b>150</b> |
| <b>Appendix B:</b> | <b>List of Acronyms.....</b>                             | <b>153</b> |
| <b>Appendix C:</b> | <b>Audit Team.....</b>                                   | <b>156</b> |
| <b>Appendix D:</b> | <b>Agency Response .....</b>                             | <b>158</b> |



---

## Section 1: Executive Summary

---

### 1.1 Background

#### 1.1.1 Purpose of this Audit

This report presents the results of an independent performance audit of the Consumer Financial Protection Bureau (CFPB) – commissioned by the CFPB in accordance with the Full-Year Continuing Appropriations Act, 2011 (Pub. L. 112-10) of April 15, 2011, Title V, Section 1573 (a) – which amended the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) to add the following text:

- (a) Annual Independent Audit.--The Bureau shall order an annual independent audit of the operations and budget of the Bureau.
- (b) Annual GAO Audit.--The Comptroller General of the United States shall conduct an annual audit of the Bureau's financial statements in accordance with generally accepted government accounting standards.

In accordance with requirement (a), the Bureau contracted with ASR Analytics (ASR) to conduct the first independent audit of the operations and budget of the Bureau in fiscal year 2011 (FY11). This report—published on October 15, 2011—focused on five areas of performance: (1) Communications and Transparency; (2) Consumer Response; (3) Human Capital and Organizational Development; (4) Information Technology; and (5) the CFPB Budget.

CFPB again contracted with ASR in FY12 to conduct the second annual independent audit of the operations and budget of the Bureau, the results of which are presented in this report. The FY12 audit focuses on three key areas of operations: (1) Privacy Programs, Policies and Processes; (2) Travel Systems and Services, including the travel card program; and (3) the CFPB Budget. In addition, as part of the FY12 audit, CFPB asked ASR to evaluate the corrective actions that the Bureau has taken to address findings and recommendations from the FY11 performance audit.

It is important to note that this is a performance audit, not a financial audit, and thus does not overlap with the Annual Government Accountability Office (GAO) Audit described in requirement (b) above. The purpose of this performance audit is to provide objective analysis that helps CFPB management to improve program performance and operations, reduce costs, facilitate decision making, and contribute to public accountability.

### 1.2 Compliance with Government Auditing Standards

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

Information for this performance audit was derived from physical evidence, documentary evidence, and testimonial evidence, most of which was provided by the CFPB. We reviewed more than 700 artifacts over the course of this study, including policy and planning documents, status reports,

briefing memos, meeting minutes, discussion decks, statements of work, and other sources. In addition, we held more than 100 meetings with CFPB personnel and other stakeholders.

## 1.3 Organization of this Report

Section 1 of this report is an Executive Summary. Sections 2 through 4 present findings and recommendations related to the three performance areas that were selected for the FY12 audit (FY12 Review Areas). Section 2 focuses on Privacy Programs, Policies and Processes; Section 3 on Travel Systems and Services; and Section 4 on the CFPB Budget.<sup>1</sup> Sections 5 through 8 examine the corrective actions that CFPB has taken in response to recommendations made in the FY11 audit. These sections relate to four areas of operations that were audited in FY11, but not repeated in FY12. We refer to these areas as FY11 Review Areas. Section 5 focuses on Communications and Transparency; Section 6 on Consumer Response; Section 7 on Human Capital and Organizational Development; and Section 8 on Information Technology. Appendix A provides a list of CFPB officials who provided input to this audit; Appendix B presents a list of acronyms used in this report; Appendix C identifies the members of our audit team; and Appendix D summarizes the agency's response to recommendations from this performance audit.

### 1.3.1 FY12 Review Areas

For each of the FY12 Review Areas, we present information on three topics: (1) audit scope; (2) evaluation criteria; and (3) findings and recommendations.<sup>2</sup> Below, we summarize the information addressed within each of these topics.

- 1. Scope of Audit.** The purpose of this section is to define the overall scope of the Review Area and to enumerate the performance elements that are within the scope of this audit. The audit scope defines the subject matter that the auditors have assessed and reported on, such as a particular business process, organizational unit, or technology system. If applicable, this section also describes any significant constraints imposed on the audit due to information limitations or other scope impairments.
- 2. Evaluation Criteria.** The purpose of this section is to establish the criteria that the ASR Team will use to evaluate CFPB's performance in the Review Area. Evaluation criteria represent the laws, regulations, standards, requirements, measures, and benchmarks against which performance is compared or evaluated. In general, our audit focuses on three sets of criteria: (1) compliance with the legal requirements; (2) achievement of organizational goals; and (3) alignment with performance standards, best practices, and/or benchmarks. These criteria are consistent with GAO standards for evaluation criteria, as published in December 2011 (GAO-12-331G, Government Auditing Standards, 2011 Revision, Section A6.02). Within each section of this report, we identify the evaluation criteria that are specific to each Review Area—and we cite specific evaluation frameworks and/or methodologies that are used to support the evaluation.

---

<sup>1</sup> Section 4 also addresses corrective actions that the Bureau has taken in response to recommendations from the FY11 audit, related to the CFPB budget.

<sup>2</sup> The Budget review area contains two sections reporting findings and recommendations—one that presents recommendations related to new review items and one that addresses corrective actions taken in response to FY11 recommendations.

- 3. Findings and Recommendations.** Within each section, we evaluate the CFPB’s performance with respect to three sets of criteria—legal requirements, organizational goals, and performance standards. Our findings and recommendations are presented in two ways. First, within the body of the report, we offer recommendations and suggestions for future action, and we describe the criteria on which these recommendations are based. Second, we present a detailed table that describes the progress that the bureau has demonstrated to date with respect to each performance criterion.

### 1.3.2 FY11 Review Areas

For each FY11 Review Area—Communications and Transparency, Consumer Response, Human Capital and Organizational Development, and Information Technology—we present information on two topics: (1) audit scope; and (2) findings and recommendations. Below, we summarize the information addressed within each of these topics.

- 1. Scope of Audit.** The purpose of this section is to define the overall scope of the Review Area and summarize the recommendations and suggestions that were made in the FY11 audit. If applicable, this section also describes any significant constraints imposed on the audit due to information limitations or other scope impairments.
- 2. Findings and Recommendations.** Findings and recommendations for FY11 Review Areas are presented in two ways. First, we provide a list of residual findings and recommendations related to performance issues identified in FY11 that require further action. Second, we present a table that summarizes the actions taken by the bureau in response to each FY11 recommendation and states whether further action is required to address the recommendation or whether the recommendation is closed.

### 1.3.3 Categorization of Recommendations

In order to assist CFPB management in prioritizing its response to recommendations contained in this report, we have categorized each new or residual recommendation based on its severity, using the categories defined below. The least severe category (Performance Improvement Opportunity) is reserved for items that do not require corrective action. Corrective action is recommended for items in the remaining five categories, which are collectively referred to as “significant performance issues”.

- **Performance Improvement Opportunity.** Corrective action is not required, but there exists the potential to improve programs, operations, and/or performance.
- **Risk of Deficiency or Noncompliance.** Corrective action is needed in order to mitigate the risk of future deficiencies in internal control, noncompliance, abuse or fraud.
- **Deficiency in Internal Control.** The design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct: (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis.

- **Noncompliance.** Performance with respect to this element is not compliant with provisions of relevant laws, regulations, contracts, and/or grant agreements.
- **Abuse.** Performance with respect to this element is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances.
- **Fraud.** Performance with respect to this element demonstrates willful misrepresentation or deception, in order to achieve financial or personal gain.

## 1.4 Summary of Findings and Recommendations

### 1.4.1 FY12 Review Areas

As described above, this audit focuses on three broad categories of evaluation criteria: (1) compliance with the legal requirements; (2) achievement of organizational goals; and (3) alignment with performance standards, best practices, and/or benchmarks. Within each of these categories, we examined various aspects of the Bureau's performance, corresponding to specific legal requirements, organizational goals, or performance standards. We refer to these specific components as "performance elements." A list of performance elements for each Review Area was initially presented in our Audit Plan deliverable.

Across the three FY12 Review Areas, we examined the Bureau's performance with respect to 61 total performance elements. The audit team provided no recommendations or suggestions for 50 of the 61 performance elements (82%), indicating that there were no significant performance issues in these areas and no identified opportunities for improvement. The remaining performance elements are addressed through 14 suggestions and recommendations, 11 of which are classified as performance improvement opportunities.<sup>3</sup> The 3 remaining recommendations are classified as significant performance issues—including 2 risks of deficiency or noncompliance and 1 instance of noncompliance. We did not identify any deficiencies in internal control, nor any instances of abuse or fraud.

### 1.4.2 FY11 Review Areas

As part of this year's performance audit, we examined actions that the Bureau has taken in response to 159 recommendations and suggestions from the FY11 report. Based on the Bureau's demonstrated performance, we assigned a status of "Closed" to 157 of the FY11 recommendations and suggestions (99%), indicating that no formal corrective action is needed. Included among these closed items are 16 performance improvement opportunities, where suggestions are provided but no corrective action is required. The remaining 2 items are classified as risks of deficiency or noncompliance, which require corrective action.

---

<sup>3</sup> Some performance elements were assigned more than one recommendation.

## Section 2: Privacy

---

### 2.1 Scope of Audit

In order to evaluate the CFPB's performance with respect to privacy, we used the *Generally Accepted Privacy Principles* (GAPP), a maturity model jointly created by the American Institute of Certified Public Accountants, Inc. (AICPA) and Canadian Institute of Chartered Accountants (CICA). The GAPP maturity model was selected for the following reasons:

- GAPP was developed by an independent task force composed of recognized privacy experts;
- GAPP is equally applicable to public and private sector organizations;
- GAPP is based on ten internationally accepted privacy principles that have been adopted as the foundation of law globally, including within the United States;
- GAPP provides explicit examples and considerations for the review of each of the criteria specified; and
- GAPP recognizes five levels of maturity within these principles. This readily identifies strategies for an organization to evolve.

The GAPP model recognizes ten principles that should be considered in a privacy program. The ten principles include<sup>4</sup>:

1. **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures, and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations, and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.

---

<sup>4</sup> Generally Accepted Privacy Principles, August 2009, American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, [http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP\\_BUS\\_%200909.pdf](http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf)

**10. Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures, and has procedures to address privacy related complaints and disputes.

Based on information found in the Privacy Office section of the CFPB website, <http://www.consumerfinance.gov/privacy-office/> (as of the date of this report), our review will focus on the major accomplishments and plans that the CFPB has listed as “commitments.” These commitments, also identified as the CFPB “privacy principles,” coincide with maturity criteria reflected in the GAPP model. The table below lists the CFPB privacy principles and the GAPP principles in which these focus areas are covered.

|   | Generally Accepted Privacy Principles (GAPP) |        |                    |            |                              |        |                             |                      |         |                            |
|---|--|--------|--------------------|------------|------------------------------|--------|-----------------------------|----------------------|---------|----------------------------|
|   | Maturity Criteria                            |        |                    |            |                              |        |                             |                      |         |                            |
| CFPB Privacy Principles                   | Management                                   | Notice | Choice and consent | Collection | Use, retention, and disposal | Access | Disclosure to third parties | Security for privacy | Quality | Monitoring and enforcement |
| Purpose of collection                     |  |        |                    | ✓          |                              |        | ✓                           |                      |         |                            |
| Openness and transparency                 | ✓  | ✓      | ✓                  | ✓          | ✓                            | ✓      | ✓                           | ✓                    | ✓       | ✓                          |
| Data minimization                         |  |        |                    | ✓          | ✓                            |        |                             |                      |         |                            |
| Limits on uses and sharing of information |  |        | ✓                  | ✓          | ✓                            |        | ✓                           |                      |         | ✓                          |
| Data quality and integrity                |  |        |                    |            |                              |        |                             |                      | ✓       |                            |
| Security                                  | ✓  |        |                    |            |                              |        | ✓                           | ✓                    |         |                            |
| Individual participation                  |  |        | ✓                  |            |                              | ✓      |                             |                      |         |                            |
| Awareness and training                    | ✓  |        |                    |            |                              |        |                             |                      |         |                            |
| Accountability and auditing               | ✓  |        |                    |            |                              |        |                             |                      |         | ✓                          |

## 2.2 Evaluation Criteria

The purpose of this section is to describe evaluation criteria for this review area. As with other areas of performance, our audit focuses on three hierarchical levels: (1) compliance with the law; (2) achievement of organizational goals; and (3) alignment with performance standards, best practices, and/or benchmarks.

### 2.2.1 Compliance with the Law

CFPB is required to comply with privacy and confidentiality requirements identified in Title X of the Dodd-Frank Act as well as other laws, regulation, and other sources of legal guidance. The bullets below cite specific provisions of the Dodd-Frank Act that establish requirements and/or evaluation criteria in the area of privacy.

- Section 1022(c)(8) of the Dodd-Frank Wall Street Reform and Consumer Protection Act addresses Privacy Considerations—citing requirements to “take steps to ensure that proprietary, personal, or confidential consumer information that is protected from public disclosure under section 552(b) or 552a of title 5, United States Code, or any other provision of law, is not made public under this title.”
- Section 1022(c)(9) of the Dodd-Frank Wall Street Reform and Consumer Protection Act addresses Consumer Privacy with regard to the collection of financial information from an individual in accordance with the Right to Financial Privacy Act of 1978.
- Section 1013(b)(3) of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires that a unit be established to collect and track consumer complaints. This unit may share information with the states as well as other Federal agencies with protections “subject to the standards applicable to Federal agencies for protection of confidentiality of personally identifiable information and for data security and integrity.”
- Section 1013(a)(5)(B) of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires that an Agency Ombudsman be established to: “(i) act as a liaison between the Bureau and any affected person with respect to any problem that such party may have in dealing with the Bureau, resulting from the regulatory activities of the Bureau; and (ii) assure that safeguards exist to encourage complainants to come forward and preserve confidentiality.”

In addition to the Dodd-Frank Wall Street Reform and Consumer Protection Act, there are a number of privacy laws and requirements that CFPB addresses. These include, but are not limited to:

**Privacy Act of 1974, 5 U.S.C. 552a.**

- Establishes standards and restrictions governing the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) about individuals, on the part of federal agencies to the extent that such PII is contained in agency systems of record.
- Requires that agencies publish notices in the Federal Register regarding the systems of record that are used to store PII, and gives individuals the ability to seek access to and amendment of their records.

**E-Government Act of 2002 (EGOV)**

- Requires agencies to maintain security programs to protect PII, commensurate with the risk and magnitude of harm due to potential unauthorized system access. (FISMA)
- Requires agencies to conduct Privacy Impact Assessments (PIAs) prior to developing or procuring IT systems that collect, maintain, or disseminate information in identifiable form.
- Requires privacy policies to be present on agency web sites. These policies are required to be present in machine readable format.

## 2.2.2 Achievement of Organizational Goals

In order to evaluate the CFPB's performance with respect to achievement of organizational goals, we examine the Bureau's progress in meeting the nine privacy commitments that are documented on the CFPB's Privacy Office web page.<sup>5</sup> The CFPB states these commitments as follows:

- **Purpose of collection:** The CFPB will state the purpose and legal authority for collecting personally identifiable information ("PII").
- **Openness and transparency:** The CFPB will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.
- **Data minimization:** The CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. The CFPB should keep PII only as long as needed to fulfill that purpose.
- **Limits on uses and sharing of information:** The CFPB will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.
- **Data quality and integrity:** The CFPB will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.
- **Security:** The CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Individual participation:** The CFPB will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate.
- **Awareness and training:** The CFPB will train all personnel about the proper treatment of PII.
- **Accountability and auditing:** The CFPB is accountable for complying with these principles.

## 2.2.3 Alignment with Performance Standards and Best Practices

We use the GAPP Maturity Model to measure performance against industry standards and to assess alignment with best practices. Within each of the GAPP principles, specific criteria have been established that are used to evaluate CFPB's performance. For example, within the Management area, GAPP establishes 14 criteria, the first of which is Privacy Policy. The description for this criterion is:

*The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.*

Each GAPP criterion is used to rate the Bureau's performance, based on a maturity scale that is consistent with expectations for an evolving organization such as the CFPB. The rating scale used within the GAPP maturity model has five levels, as described below:

1. **Ad Hoc** – procedures or processes are generally informal, incomplete, and inconsistently applied.

---

<sup>5</sup> <http://www.consumerfinance.gov/privacy-office/>

2. **Repeatable** – procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
3. **Defined** – procedures and processes are fully documented and implemented, and cover all relevant aspects.
4. **Managed** – reviews are conducted to assess the effectiveness of the controls in place.
5. **Optimized** – regular review and feedback are used to ensure continuous improvement towards optimization of the given process.

The GAPP maturity model specifies characteristics that would be evidenced in each of the different maturity levels, or each criterion. Returning to the example of privacy policies, the characteristics for each maturity level are listed below:

1. **Ad Hoc** - Some aspects of privacy policies exist informally.
2. **Repeatable** - Privacy policies exist but may not be complete, and are not fully documented.
3. **Defined** - Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.
4. **Managed** - Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.
5. **Optimized** - Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.

In order to summarize the current state of privacy policies and procedures at CFPB, individual ratings are provided for each GAPP criterion, reflecting the Bureau's accomplishments to date.

The guidance provided by the GAPP framework has been supplemented by various publications, research, and tools from the International Association of Privacy Professionals (IAPP), whose web site may be found at <https://www.privacyassociation.org/>. Relevant publications include, but are not limited to:

- Building a Privacy Program - A Practitioner's Guide
- U.S. Government Privacy : Essential Policies and Practices for Privacy Professionals
- Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices

## 2.3 Findings and Recommendations

In this section, we present findings and recommendations related to CFPB's performance in the area of Privacy. In general, we found that the Bureau has established policies and procedures in this area that comply with legal requirements, support organizational goals, and align with generally accepted performance standards and best practices. Although the Chief Privacy Officer and the Privacy Team have been in place for just over one year—during this time, they have laid the foundation for a robust privacy program, by focusing on the mandatory requirements for this discipline.

Most notably, a culture of privacy has been established that is supported by executive management and reinforced by an extensive awareness and training program. Overall, the CFPB privacy program

has established a set of Repeatable practices based on the GAPP Maturity Model, which is acceptable and appropriate for a program this young.

Within the Privacy review area, we examined the Bureau's performance with respect to 26 total performance elements. The audit team provided no recommendations or suggestions for 19 of the 26 performance elements (73%), indicating that there were no significant performance issues in these areas and no identified opportunities for improvement. The remaining performance elements are addressed through 10 suggestions and recommendations, 7 of which are classified as performance improvement opportunities.<sup>6</sup> The 3 remaining recommendations are classified as significant performance issues—including 2 risks of deficiency or noncompliance and 1 instance of noncompliance. We did not identify any deficiencies in internal control, nor any instances of abuse or fraud.

### 2.3.1 Significant Performance Issues

Below, we state our findings and recommendations related to 3 significant performance issues in the Privacy area. For each, we document: (1) the categorization of the performance issue (i.e., risk of deficiency or noncompliance, deficiency in internal control, noncompliance, abuse, or fraud); (2) the criteria, condition, cause, and effect associated with the performance issue; and (3) our recommendations for addressing the performance issue.<sup>7</sup>

**2012.PR.1.2 Establishment of a machine readable privacy notice on CFPB website (Noncompliance).** The E-Government Act of 2002 (EGOV) requires that privacy policies be present on agency web sites and that these policies be available in machine-readable format. The CFPB website currently contains high-level notices describing the CFPB Privacy Principles and references to SORNs for additional details, but these notices are not in machine-readable format. Without a machine-readable policy the privacy preferences set by visitors in their browsers will be ignored when CFPB's pages are rendered. We recommend that CFPB establish a machine readable privacy notice on its website.

**Agency Response.** The Bureau concurs with this recommendation and is in the process of determining how to satisfy the "machine readable privacy policy" requirement in a way that aligns with the Bureau's values of technology and user-friendly innovation. The Bureau's goal is to be in compliance with the requirement under the law. As noted by ASR, the Bureau has a clear and easily accessible privacy policy posted on its website which informs users of the manner in which the Bureau handles privacy issues, including the use of cookies. The policy, per federal guidance, directs visitors to instructions on how to disable or modify their browser's acceptance of cookies. Like all modern sites, ConsumerFinance.gov respects a user's browser settings relative to how and when cookies should be accepted. Moreover, the CFPB website does not actively collect personally identifiable information (PII) without users' express consent; rather, users may choose to give consent and provide PII, as stated in CFPB policy. The Bureau has also published a Privacy Impact Assessment

---

<sup>6</sup> Some performance elements were assigned more than one recommendation.

<sup>7</sup> Throughout this report, we use an alphanumeric ID code to uniquely identify each recommendation and suggestion. The ID code is a concatenation of text that describes the year of the report in which the recommendation was made (e.g., 2011), the review area (e.g., PR for Privacy), and a hierarchical numeric code (e.g., 1.1). In cases where multiple recommendations are presented on the same topic, alpha characters may be added to the numeric code (e.g., 1.1a, 1.1b, 1.1c).

(PIA) about ConsumerFinance.gov. Therefore, there is little risk to consumers or others visiting ConsumerFinance.gov posed by the website's existing configuration at this time.

**2012.PR.2.3 Approval of CFPB Privacy Policy (Risk of Deficiency or Noncompliance).** OMB memorandum M-07-16 dated May 27, 2007 discusses agency responsibilities in protecting against the breach of personally indefinable information aiding in the protection of privacy. With regard to the establishment of policies for rules and consequences related to protecting personally identifiable information, Attachment 4, section A specifies:

*...it is the responsibility of each agency head to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.*

The Privacy Team has developed and communicated a Bureau-wide Privacy Policy for all CFPB systems and processes in alignment with applicable laws, regulations, and standards. While the current policy is awaiting final approval, the Privacy Team and others are operating as if approval has been achieved. We recommend that the formal approval process be completed for the Privacy Policy.

**Agency Response.** The Bureau's assessment is that this recommendation represents an opportunity for performance improvement and there exists no risk of deficiency or noncompliance. The only legally required policy related to privacy is the website privacy policy, which has been available from the time ConsumerFinance.gov went live. Under Section 1017(a)(4)(E) of the Consumer Financial Protection Act, the CFPB is generally not required to follow OMB guidance or consult with or obtain the approval of OMB with respect to Bureau affairs or operations. Therefore, the Bureau does not believe corrective action is required to mitigate the risk of future non-compliance or deficiency.

The Privacy Team is in the process of expanding and supplementing its program with additional policies and procedures to enhance the basic program, even though these are not legally required. Accordingly, the Privacy Team expects to finalize and implement both a Bureau-wide privacy policy and, in coordination with the Chief Information Security Officer, an acceptable use of technology policy in the normal course of operations.

**2012.PR.3.2 Bi-annual review of SORNs and PIAs (Risk of Deficiency or Noncompliance).** In accordance with GAPP privacy principles, the Bureau should provide notice about its privacy policies and procedures, and identify the purposes for which personal information is collected, used, retained, and disclosed. A high level privacy notice does appear on the CFPB website; the notice is written in clear, easy to understand language; and additional details are provided through SORNs and PIAs. However, there is no formal policy to revisit the SORNs and PIAs after the implementation of a system is complete. We recommend that all systems be reviewed at least bi-annually to identify any changes that may require changes to the notice.

**Agency Response.** The Bureau's assessment is that this recommendation represents an opportunity for performance improvement and there exists no risk of deficiency or noncompliance. The Privacy Team has plans to review and validate SORNs and PIAs every two years. Under Section 1017(A)(4)(e) of the Consumer Financial Protection Act, the CFPB generally is not required to follow OMB guidance or consult with or

obtain the approval of OMB with respect to Bureau affairs or operations, although the Bureau recognizes the procedures in Appendix I of OMB Circular A-130 as best practices. Although procedures are not yet documented, the Privacy Team is aware of and is current in its review obligations. Of the 23 SORNs and PIAs in place during the time of this audit, the Privacy Team has republished three and notes that the vast majority of the remainder are less than one year old and, therefore, will not come up for review until 2013 and 2014. The policies documenting such reviews will be included in the Bureau's guidance on SORNs and PIAs. The Privacy Team will formalize these policies and procedures as the Bureau matures.

### **2.3.2 Performance Improvement Opportunities**

Below, we present information on 6 aspects of performance that we believe could be improved, but do not require corrective action. For each of these performance improvement opportunities, we offer suggestions for future action, and we summarize the criteria on which these suggestions are based.

**2012.PR.1.1 “Blanket routine uses” for internal SORNs.** The Privacy Act of 1974, 5 U.S.C. 552a, requires that agencies publish notices in the Federal Register regarding the systems of record that are used to store PII. CFPB's Privacy Team has completed SORNs and PIAs for most systems. We recommend that the CFPB write and publish “blanket routine uses” for their internal SORNs. These “blanket routine uses” would specify a single notice for common information and processes used across all CFPB systems. The “blanket routine uses” would be published only once, as a preface to all of the CFPB SORNs in the interest of simplicity, economy, and to avoid redundancy. They would apply to all of the CFPB's SORNs and are compatible with the purpose for which the information was originally collected.

**2012.PR.2.1 Definition of data retention periods for each system.** In accordance with CFPB privacy principle of Data Minimization, the CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. Members of the Privacy Team are involved with systems design ensuring data collected is restricted to information required to address stated objectives. However, data retention periods have not yet been defined across all information collected. Although these may be several years off, we recommend that data retention periods should be defined as a requirement during the design of each system.

**2012.PR.2.2 Development of a plan for the formal definition of policies and procedures used to protect PII.** In accordance with the CFPB privacy principle of Security, the CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. CFPB relies on many of the Treasury Department's processes and procedures for the security of personal information. CFPB is becoming independent of the services provided by the Treasury Department in the first half of 2013, according to CFPB's Chief Information Officer. Discussions with members of the Security and Privacy teams indicate that there is an objective to define policies and procedures for this new independent state, however a formal plan for defining those policies and procedures has not been developed. We recommend that a plan be developed so that the applicable Treasury policies and procedures should be adopted or adapted to meet CFPB's requirements prior to the independent systems going live.

**2012.PR.2.4 Approval of CFPB privacy-related policies and procedures.** In addition to the core Privacy Policy, discussed above in recommendation 2012.PR.2.3, the Privacy Team is responsible for developing and communicating supplemental Bureau-wide Privacy policy, guidance, and

requirements for all CFPB systems in alignment with applicable laws, regulations, and standards. Many of these policies and procedures are in draft form awaiting approval. The utilization of undocumented or unapproved policies and/or procedures does not guarantee the uniform application of practices within the organization. While the Privacy Team and others are operating as if approval has been achieved, we recommend that the approval process be completed for each of the outstanding items, including but not limited to the Policy for Managing and Protecting CFPB Sensitive System Data Extracts, Enterprise Information Systems Security Policy, Incident Response Plan, Baseline Privacy Requirements, Guidance for Privacy Act Statements, and Standard Operating Procedures: Personally Identifiable Information (PII) Breaches.

**2012.PR.2.5 Participation of Chief Privacy Officer in review of contracts involving personal information.** In accordance with the CFPB privacy principle of Accountability and Auditing, the Bureau is accountable for complying with its privacy principles. To this end, members of the Privacy Team are assigned to work with other departments of the Bureau, to ensure that the Privacy Team actively participates in the definition of requirements for new projects or changes to existing processes. However, the Privacy Team does not participate in the review of contracts where personal information is involved. We recommend that the Chief Privacy Officer participate in this review process.

**2012.PR.3.1 Layered presentation of privacy information in CFPB website privacy notice.** In accordance with GAPP privacy principles, the Bureau should provide notice about its privacy policies and procedures, and identify the purposes for which personal information is collected, used, retained, and disclosed. A high level privacy notice appears on the CFPB website, and this high level notice is written in clear, easy to understand language. Additional details are provided by the SORNs and PIAs. Best practices for privacy notices have evolved to allow for a layered presentation of information. This permits a reader to gather the most pertinent information in a high level notice and then drill down into more detailed documents if they desire. We recommend that information be added to the high level privacy statement currently available on the CFPB web site that summarizes the information that are contained in the SORNs / PIAs such as a summary of what PII is collected.

**2012.PR.3.3 Establishment of formal privacy compliance program.** In accordance with GAPP privacy principles, the Bureau should monitor compliance with its privacy policies and procedures, and have procedures to address privacy related complaints and disputes. Currently, the Bureau uses informal processes to monitor compliance with privacy practices. We recommend that a formal compliance program be established for CFPB employees, contractors, and other parties that may have access to PII.

### **2.3.3 Summary of Demonstrated Performance**

Table 1 presents information on the Bureau's demonstrated performance and achievements across all 26 performance elements that were audited in this review area.

**Table 1: Summary of Demonstrated Performance**

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity  |
|---|--|--|
| <b>Compliance with the Law</b>  |  |  |
| <p>Section 1022(c)(8) of the Dodd-Frank Wall Street Reform and Consumer Protection Act addresses Privacy Considerations—citing requirements to “take steps to ensure that proprietary, personal, or confidential consumer information that is protected from public disclosure under section 552(b) or 552a of title 5, United States Code, or any other provision of law, is not made public under this title.”</p>                                | <ul style="list-style-type: none"> <li>• Personal information is protected by processes defined with the participation of the CFPB Privacy Team.</li> <li>• Access to personal information for CFPB is coordinated through the FOIA office.</li> <li>• Processes exist to review these requests which include review by the Chief Privacy Officer as necessary.</li> <li>• CFPB has established as a Data Coordination Council that reviews requests for sharing information with other Federal Agencies and states ensuring proper confidentiality, security, and integrity standards are maintained."</li> </ul> | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
| <p>Section 1022(c)(9) of the Dodd-Frank Wall Street Reform and Consumer Protection Act addresses Consumer Privacy with regard to the collection of financial information from an individual or service provider in accordance with the Right to Financial Privacy Act of 1978.</p>  | <ul style="list-style-type: none"> <li>• The CFPB Enforcement Team addresses requests for information from financial institutions.</li> <li>• The Enforcement Team has been reported to follow procedures used by agencies that previously performed these checks.</li> <li>• The Privacy Team is not currently involved in this area.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
| <p>Section 1013(b)(3) of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires that a unit be established to collect and track consumer complaints. This unit may share information with the states as well as other Federal agencies with protections “subject to the standards applicable to Federal agencies for protection of confidentiality of personally identifiable information and for data security and integrity.”</p> | <ul style="list-style-type: none"> <li>• CFPB has established a Data Coordination Council that reviews requests for sharing information with other Federal Agencies and states, ensuring proper confidentiality, security, and integrity standards are maintained.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity  |
|---|--|--|
| <p>Section 1013(a)(5)(B) of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires that an Agency Ombudsman be established to: "(i) act as a liaison between the Bureau and any affected person with respect to any problem that such party may have in dealing with the Bureau, resulting from the regulatory activities of the Bureau; and (ii) assure that safeguards exist to encourage complainants to come forward and preserve confidentiality."</p>   | <ul style="list-style-type: none"> <li>• The Agency Ombudsman follows the procedures recommended by the Privacy Team to preserve confidentiality. Policies and procedures have been defined in a February 2012 memo that presents the foundation for a "living document." As improvements to the policies and procedures are identified, the document is updated and/or supplemented.</li> </ul>   | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |
| <p>The Privacy Act of 1974, 5 U.S.C. 552a, requires that agencies publish notices in the Federal Register regarding the systems of record that are used to store PII, and gives individuals the ability to seek access to and amendment of their records.</p>   | <ul style="list-style-type: none"> <li>• CFPB's Privacy Team has established standards and restrictions on the maintenance, use, and dissemination of PII.</li> <li>• SORNs and PIAs have been completed satisfactorily for most systems and may be found at <a href="http://www.consumerfinance.gov/privacy-office/">http://www.consumerfinance.gov/privacy-office/</a></li> <li>• Individuals may access and amend their PII through FOIA processes, as documented on the CFPB web site."</li> </ul> | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |
| <p>The Privacy Act of 1974, 5 U.S.C. 552a, establishes standards and restrictions governing the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) about individuals, on the part of federal agencies to the extent that such PII is contained in agency systems of record. The act also requires that agencies publish notices in the Federal Register regarding the systems of record that are used to store PII, and gives individuals the ability to seek access to and amendment of their records.</p> | <ul style="list-style-type: none"> <li>• CFPB's Privacy Team has established standards and restrictions on the maintenance, use, and dissemination of PII.</li> <li>• SORNs and PIAs have been completed satisfactorily for most systems and may be found at <a href="http://www.consumerfinance.gov/privacy-office/">http://www.consumerfinance.gov/privacy-office/</a></li> <li>• Individuals may access and amend their PII through FOIA processes, as documented on the CFPB web site.</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.PR.1.1 (Performance Improvement Opportunity): We recommend that the CFPB write and publish "blanket routine uses" for their internal SORNs. These "blanket routine uses" would specify a single notice for common information and processes used across all CFPB systems. The "blanket routine uses" would be published only once, as a preface to all of the CFPB SORNs in the interest of simplicity, economy, and to avoid redundancy. They would apply to all of the CFPB's SORNs and are compatible with the purpose for which the information was originally collected.</p> |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Performance Improvement Opportunity  |
|---|---|--|
| <p>The E-Government Act of 2002 (EGOV):<br/>                     Requires agencies to maintain security programs to protect PII, commensurate with the risk and magnitude of harm due to potential unauthorized system access. (FISMA)<br/>                     Requires agencies to conduct Privacy Impact Assessments (PIAs) prior to developing or procuring IT systems that collect, maintain, or disseminate information in identifiable form.<br/>                     Requires privacy policies to be present on agency web sites. These policies are required to be present in machine readable format.</p> | <ul style="list-style-type: none"> <li>CFPB has created a security program to protect against unauthorized system access. The performance of this program was audited in 2011. PIAs have been completed satisfactorily for most systems and may be found at <a href="http://www.consumerfinance.gov/privacy-office/">http://www.consumerfinance.gov/privacy-office/</a><br/>                     High level notices describing the CFPB Privacy Principles are provided on the website but are not in machine-readable format.</li> </ul> | <p>Additional Action Required</p> <p>2012.PR.1.2 (Noncompliance): We recommend that CFPB should establish a machine readable privacy notice on the website.</p>  |
| <p><b>Achievement of Organizational Goals</b></p>   |   |  |
| <p>Purpose of collection: The CFPB will state the purpose and legal authority for collecting personally identifiable information ("PII").</p>   | <ul style="list-style-type: none"> <li>The CFPB provides the purpose and legal authority for collecting PII in SORNs and PIAs. CFPB systems are not made operational until the related SORNs / PIAs have been completed</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |
| <p>Openness and transparency: The CFPB will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.</p>   | <ul style="list-style-type: none"> <li>The CFPB provides a high level privacy statement on the website at <a href="http://www.consumerfinance.gov/privacy-policy/">http://www.consumerfinance.gov/privacy-policy/</a></li> <li>Further details are provided within the SORNs/PIAs for individual systems.</li> <li>At the time a complaint is being filed on-line a concise summary of the privacy notice is provided.</li> </ul>   | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |
| <p>Data minimization: The CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. The CFPB should keep PII only as long as needed to fulfill that purpose.</p>   | <ul style="list-style-type: none"> <li>Members of the Privacy Team are involved with systems design ensuring data collected is restricted to information required to address stated objectives.</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.PR.2.1 (Performance Improvement Opportunity): Data retention periods have not yet been defined across all information collected. Although these may be several years off, we recommend that data retention periods should be defined as a requirement during the design of each system.</p> |

| Performance Requirement or Standard  | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity  |
|--|--|--|
| <p>Limits on uses and sharing of information: The CFPB will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.</p> | <ul style="list-style-type: none"> <li>Guidelines for the dissemination of information by CFPB may be found at <a href="http://www.consumerfinance.gov/informationquality/">www.consumerfinance.gov/informationquality/</a></li> <li>The Data Coordination Council reviews requests for sharing of information. The Privacy Team has an active role on this council.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
|  | <ul style="list-style-type: none"> <li>The Data Coordination Council reviews requests for sharing of information. The Privacy Team has an active role on this council.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
| <p>Data quality and integrity: The CFPB will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.</p>  | <ul style="list-style-type: none"> <li>The Consumer Financial Protection Bureau (Bureau) Information Quality Guidelines are issued in accordance with the provisions of the Treasury and General Government Appropriations Act for fiscal year 2001, Pub. L. No. 106-554, and OMB government-wide guidance.</li> <li>CFPB is dependent upon the originator of PII data (e.g., citizens, banks, other government agencies, third parties) to ensure the quality of the information.</li> <li>When data supplied to CFPB is corrected, the correction is provided to the originating source. A reciprocal agreement is required when CFPB supplies information to others.</li> </ul> | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity  |
|---|--|--|
| <p>Security: The CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.</p>                           | <ul style="list-style-type: none"> <li>• CFPB relies on many of the Treasury Department's processes and procedures for the security of personal information.</li> <li>• Security assessments have been done for the cloud providers currently in use.</li> <li>• Mobile devices are required to be encrypted by policy.</li> <li>• There is a high level of coordination and cooperation between the Security and Privacy teams</li> </ul>   | <p>Additional Action Suggested</p> <p>2012.PR.2.2 (Performance Improvement Opportunity): CFPB is becoming independent of the services provided by the Treasury Department in the first half of 2013 according to CFPB's Chief Information Officer. Discussions with members of the Security and Privacy teams indicate that there is an objective to define policies and procedures for this new independent state, however a formal plan for defining those policies and procedures has not been developed. We recommend that a plan be developed so that the applicable Treasury policies and procedures should be adopted or adapted to meet CFPB's requirements prior to the independent systems going live.</p> |
| <p>Individual participation: The CFPB will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate</p> | <ul style="list-style-type: none"> <li>• The CFPB has well defined processes for addressing concerns of individuals with regard to personal information collected.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |
| <p>Awareness and training: The CFPB will train all personnel about the proper treatment of PII.</p>   | <ul style="list-style-type: none"> <li>• The CFPB Privacy Team has established an awareness and training program that provides both generic privacy training as well as training geared toward specific business requirements.</li> <li>• Employees of CFPB are required to participate in on-line privacy training. A process is in place to address situations where employees are non-compliant with training requirements.</li> <li>• Privacy training information is contained within the Required Training in the periodic review of the Privacy program.</li> </ul> | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Performance Improvement Opportunity   |
|---|---|---|
| <p>Accountability and auditing: The CFPB is accountable for complying with these principles.</p>                                    | <ul style="list-style-type: none"> <li>The Privacy Team “develops and communicates Bureau-wide Privacy policy, guidance, and requirements for all CFPB systems in alignment with applicable laws, regulations, and standards.”</li> <li>Members of the Privacy Team are assigned to work with specific departments to ensure that the Privacy Team understands the operations and plans.</li> <li>Privacy Team members actively participate in the definition of requirements for new projects or changes to existing processes.</li> </ul> | <p>Additional Action Suggested</p> <p>2012.PR.2.4 (Performance Improvement Opportunity): Many policies and procedures are in draft form awaiting approval. The Privacy Team is operating as if approval has been achieved. We recommend that the approval process be completed for each of the outstanding items including but not limited to the Privacy Policy, Policy for Managing and Protecting CFPB Sensitive System Data Extracts, Enterprise Information Systems Security Policy, Incident Response Plan, Baseline Privacy Requirements, Guidance for Privacy Act Statements, and Standard Operating Procedures: Personally Identifiable Information (PII) Breaches.</p> <p>2012.PR.2.5 (Performance Improvement Opportunity): The Privacy Team does not participate in the review of contracts where personal information is involved. We recommend that the Chief Privacy Officer participate in this review process.</p> |
| <p><b>Alignment with Performance Standards and Best Practices</b></p>   |   |   |
| <p>Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.</p> | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) Privacy initiatives have senior management support and oversight;</li> <li>(2) Members of the Privacy Team are sufficiently qualified and trained;</li> <li>(3) Reasonable awareness and training programs are in place;</li> <li>(4) Notices are available for all but four systems of record.</li> </ul>   | <p>Additional Action Required</p> <p>2012.PR.2.3 (Risk of Deficiency or Noncompliance): A formal Privacy Policy is in draft form. We recommend that the review and approval of the formal Privacy Policy be completed.</p>  |

| Performance Requirement or Standard  | Demonstrated Performance  | Recommendation or Performance Improvement Opportunity  |
|--|---|--|
| <p>Notice. The entity provides notice about its privacy policies and procedures, and identifies the purposes for which personal information is collected, used, retained, and disclosed.</p>                 | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) A high level privacy notice appears on the CFPB website at <a href="http://www.consumerfinance.gov/privacy-policy/">http://www.consumerfinance.gov/privacy-policy/</a>;</li> <li>(2) the high level notice is written in clear, easy to understand language;</li> <li>(3) additional details are provided by the SORNs and PIAs whose links may be found at <a href="http://www.consumerfinance.gov/privacy-office/">http://www.consumerfinance.gov/privacy-office/</a></li> </ul> | <p>Additional Action Suggested</p> <p>2012.PR.3.1 (Performance Improvement Opportunity): Best practices for privacy notices have evolved to allow for a layered presentation of information. This permits a reader to gather the most pertinent information in a high level notice and then drill down into more detailed documents if they desire. We recommend that information be added to the high level privacy statement currently available on the CFPB web site that summarizes the information that are contained in the SORNs / PIAs such as a summary of what PII is collected.</p> <p>Additional Action Required</p> <p>2012.PR.3.2 (Risk of Deficiency or Noncompliance): There is no formal policy to revisit the implementation of a system once a SORN or PIA is complete. We recommend that all systems be reviewed at least bi-annually to identify any changes that may require changes to the notice</p> |
| <p>Choice and consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information</p> | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) A high level privacy notice expresses that all information is provided voluntarily to the website indicating that implied consent is operative;</li> <li>(2) An explanation is provided for collection of web traffic information with instructions of how to opt out of this collection.</li> </ul>   | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |
| <p>Collection. The entity collects personal information only for the purposes identified in the notice.</p>  | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) Members of the Privacy Team are involved with systems design ensuring data collected is restricted to information required to address stated objectives.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>   |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity  |
|---|--|--|
| <p>Use, retention, and disposal. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations, and thereafter appropriately disposes of such information.</p> | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) The Data Coordination Council reviews requests for sharing of information. The Privacy Team has an active role on this council;</li> <li>(2) Members of the Privacy Team are involved with systems design ensuring data collected is restricted to information required to address stated objectives;</li> <li>(3) Instructions are available for the proper destruction of paper-based information.</li> </ul> | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
| <p>Access. The entity provides individuals with access to their personal information for review and update.</p>   | <p>Key Accomplishments: With the FOIA team, processes have been put in place to:</p> <ul style="list-style-type: none"> <li>(1) Respond to requests for information;</li> <li>(2) Monitor the status of the responses;</li> <li>(3) Provide responses in writing to individuals requesting access.</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
| <p>Disclosure to third parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.</p>  | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) Individuals are notified in the high level Privacy notice that their information may be shared;</li> <li>(2) Legal counsel reviewing contracts is aware of privacy requirements</li> </ul>  | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |
| <p>Security for privacy. The entity protects personal information against unauthorized access (both physical and logical).</p>  | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) CFPB relies on many of the Treasury Department's processes and procedures for the security of personal information;</li> <li>(2) Security assessments have been done for the cloud providers currently in use;</li> <li>(3) Mobile devices are required to be encrypted by policy;</li> <li>(4) There is a high level of coordination and cooperation between the Security and Privacy teams.</li> </ul>        | <p>No recommendation or performance improvement opportunity identified for this performance element.</p> |

| Performance Requirement or Standard  | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity   |
|--|--|---|
| <p>Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.</p>  | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) Individuals are informed of the importance of providing accurate information as well as the mechanisms for making corrections if necessary;</li> <li>(2) When data supplied to CFPB is corrected, the correction is provided to the originating source. A reciprocal agreement is required when CFPB supplies information to others.</li> </ul> | <p>No recommendation or performance improvement opportunity identified for this performance element.</p>  |
| <p>Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures, and has procedures to address privacy related complaints and disputes.</p> | <p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>(1) Citizens are informed about how to raise inquires, complaints, and disputes;</li> <li>(2) Documented processes exist for addressing these items.</li> </ul>   | <p>Additional Action Suggested<br/>                 2012.PR.3.3 (Performance Improvement Opportunity): Monitoring compliance with privacy practices is informal. We recommend that a formal compliance program be established for CFPB employees, contractors, and other parties that may have access to PII.</p> |

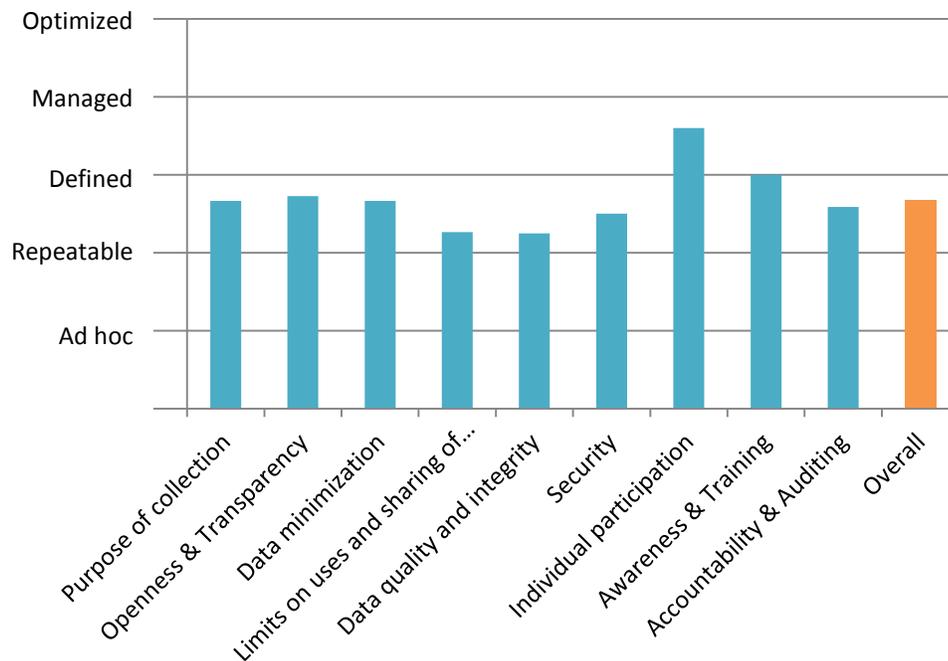
### 2.3.4 Privacy Maturity

The GAPP Maturity Model is the framework used to measure CFPB’s performance with respect to privacy. The criteria used within the GAPP model are grouped into principles allowing privacy maturity to be measured in each principle area (see section 2.3.1.1).

CFPB has identified Privacy Principles within their privacy practice. As part of this audit, the criteria included in the GAPP Maturity Model were reclassified according to CFPB Privacy Principle—allowing the maturity of the CFPB privacy program to be measured within each principle area (see section 2.3.1.2).

#### 2.3.4.1 CFPB Privacy Principle Maturity

Section 2.1 of this document provides an explanation of the CFPB Privacy Principles. The criteria used in the GAPP model have been reclassified to identify the applicable CFPB Privacy Principle. The details of the reclassification may be found within Table 2. The following chart reflects the maturity level for each of the CFPB principal areas contained in the model.

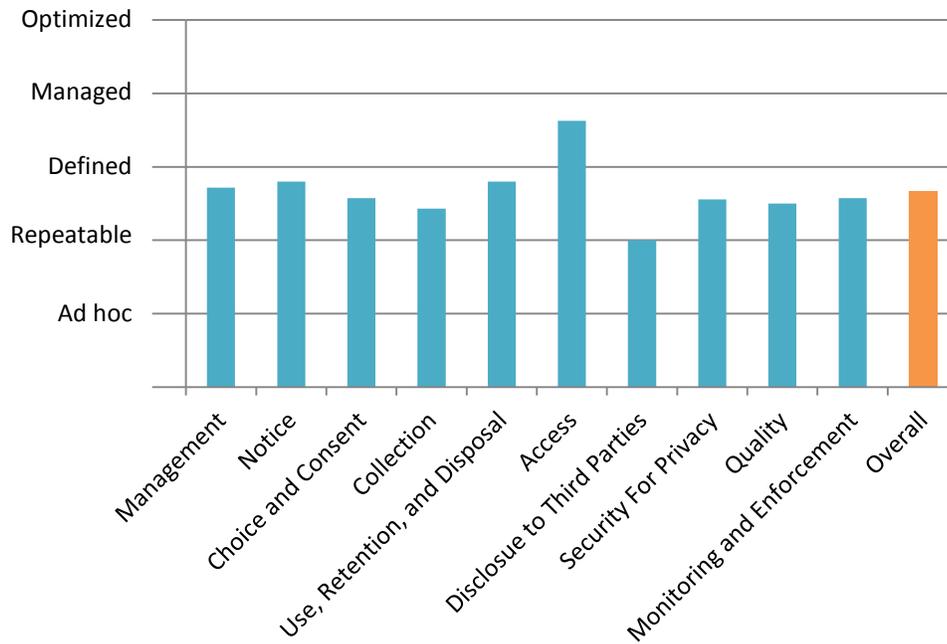


#### 2.3.4.2 Generally Accepted Privacy Practices Maturity

Section 2.1 of this document provides an explanation of the GAPP framework. Overall, the CFPB privacy program has established a set of Repeatable practices based on the GAPP Maturity Model (i.e., maturity level 2 of 5). Given the focus on mandatory requirements by the Privacy Team, this is an appropriate and acceptable result for a program this young.

Table 2 contains the maturity level for each of the principle areas used in the GAPP Maturity model. The chart below reflects CFPB’s current maturity level for each of the principal areas contained in the

model. Given the focus on mandatory requirements by the Privacy Team, this is an appropriate and acceptable result for a program this young.



**Table 2: Alignment with GAPP Maturity Model**

| GAPP Criteria                               | Criteria Description  | CFPB Principle          | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined  | Managed  | Optimized  |  |
|---|---|-------------------------|---------------------|------------|---|--|--|--|--|
| <b>MANAGEMENT (14 Criteria)</b>             | The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.  |                         |                     |            |   |  |  |  |  |
| Privacy Policies (1.1.0)                    | The entity defines and documents its privacy policies with respect to notice; choice and consent; collection; use, retention and disposal; access; disclosure to third parties; security for privacy; quality; and monitoring and enforcement.  | Openness & Transparency | 2                   | Repeatable | Some aspects of privacy policies exist informally.  | Privacy policies exist but may not be complete, and are not fully documented.  | Policies are defined for: notice, choice and consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring and enforcement.    | Compliance with privacy policies is monitored and the results of such monitoring are used to reinforce key privacy messages.         | Management monitors compliance with policies and procedures concerning personal information. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion.                         |
| Communicating to Internal Personnel (1.1.1) | Privacy policies and the consequences of non-compliance with such policies are communicated, at least annually, to the entity's internal personnel responsible for collecting, using, retaining and disclosing personal information. Changes in privacy policies are communicated to such personnel shortly after the changes are approved. | Awareness & Training    | 3                   | Defined    | Employees may be informed about the entity's privacy policies; however, communications are inconsistent, sporadic and undocumented. | Employees are provided guidance on the entity's privacy policies and procedures through various means; however, formal policies, where they exist, are not complete. | The entity has a process in place to communicate privacy policies and procedures to employees through initial awareness and training sessions and an ongoing communications program. | Privacy policies and the consequences of non-compliance are communicated at least annually; understanding is monitored and assessed. | Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback. Changes in privacy policies are communicated to personnel shortly after the changes are approved. |

| GAPP Criteria  | Criteria Description   | CFPB Principle            | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined   | Managed  | Optimized   |  |
|--|--|---------------------------|---------------------|------------|--|---|--|---|--|
| Responsibility and Accountability for Policies (1.1.2)                           | Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.                          | Accountability & Auditing | 4                   | Managed    | Management is becoming aware of privacy issues but has not yet identified a key sponsor or assigned responsibility. Privacy issues are addressed reactively. | Management understands the risks, requirements (including legal, regulatory and industry) and their responsibilities with respect to privacy. There is an understanding that appropriate privacy management is important and needs to be considered. Responsibility for operation of the entity's privacy program is assigned; however, the approaches are often informal and fragmented with limited authority or resources allocated. | Defined roles and responsibilities have been developed and assigned to various individuals / groups within the entity and employees are aware of those assignments. The approach to developing privacy policies and procedures is formalized and documented. | Management monitors the assignment of roles and responsibilities to ensure they are being performed, that the appropriate information and materials are developed and that those responsible are communicating effectively. Privacy initiatives have senior management support. | The entity (such as a committee of the board of directors) regularly monitors the processes and assignments of those responsible for the progress to determine its effectiveness. Where required, changes and improvements are made in a timely and effective fashion. |
| Review and Approval (1.2.1)  | Privacy policies and procedures, and changes thereto, are reviewed and approved by management.   | Accountability & Auditing | 4                   | Managed    | Reviews are informal and not undertaken on a consistent basis.   | Management undertakes periodic review of privacy policies and procedures; however, little guidance has been developed for such reviews.   | Management follows a defined process that requires their review and approval of privacy policies and procedures.   | The entity has supplemented management review and approval with periodic reviews by both internal and external privacy specialists.   | Management's review and approval of privacy policies also include periodic assessments of the privacy program to ensure all changes are warranted, made and approved; if necessary, the approval process will be revised.  |
| Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2) | Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made.<br><br>Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations. | Accountability & Auditing | 2                   | Repeatable | Reviews and comparisons with applicable laws and regulations are performed inconsistently and are incomplete.  | Privacy policies and procedures have been reviewed to ensure their compliance with applicable laws and regulations; however, documented guidance is not provided.   | A process has been implemented that requires privacy policies to be periodically reviewed and maintained to reflect changes in privacy legislation and regulations; however, there is no proactive review of legislation.                                    | Changes to privacy legislation and regulations are reviewed by management and changes are made to the entity's privacy policies and procedures as required. Management may subscribe to a privacy service that regularly informs them of such changes.                          | Management assesses the degree to which changes to legislation are reflected in their privacy policies.  |

| GAPP Criteria   | Criteria Description  | CFPB Principle            | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined  | Managed   | Optimized   |   |
|---|---|---------------------------|---------------------|------------|---|--|---|---|---|
| Personal Information Identification and Classification (1.2.3)          | The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified. Such information is covered by the entity's privacy and related security policies and procedures. | Accountability & Auditing | 3                   | Defined    | The identification of personal information is irregular, incomplete, inconsistent, and potentially out of date. Personal information is not adequately addressed in the entity's privacy and related security policies and procedures. Personal information may not be differentiated from other information. | Basic categories of personal information have been identified and covered in the entity's security and privacy policies; however, the classification may not have been extended to all personal information. | <b>All personal information collected, used, stored and disclosed within the entity has been classified and risk rated.</b>   | All personal information is covered by the entity's privacy and related security policies and procedures. Procedures exist to monitor compliance. Personal information records are reviewed to ensure appropriate classification. | Management maintains a record of all instances and uses of personal information. In addition, processes are in place to ensure changes to business processes and procedures and any supporting computerized systems, where personal information is involved, result in an updating of personal information records. Personal information records are reviewed to ensure appropriate classification. |
| Risk Assessment (1.2.4)   | A risk assessment process is used to establish a risk baseline and, at least annually, to identify new or changed risks to personal information and to develop and update responses to such risks.  | Security                  | 2                   | Repeatable | Privacy risks may have been identified, but such identification is not the result of any formal process. The privacy risks identified are incomplete and inconsistent.<br><br>A privacy risk assessment has not likely been completed and privacy risks not formally documented.                              | <b>Employees are aware of and consider various privacy risks. Risk assessments may not be conducted regularly, are not part of a more thorough risk management program and may not cover all areas.</b>      | Processes have been implemented for risk identification, risk assessment and reporting. A documented framework is used and risk appetite is established.<br><br>For risk assessment, organizations may wish to use the AICPA/CICA Privacy Risk Assessment Tool. | Privacy risks are reviewed annually both internally and externally.<br><br>Changes to privacy policies and procedures and the privacy program are updated as necessary.   | The entity has a formal risk management program that includes privacy risks which may be customized by jurisdiction, business unit or function. The program maintains a risk log that is periodically assessed. A formal annual risk management review is undertaken to assess the effectiveness of the program and changes are made where necessary. A risk management plan has been implemented.  |
| Consistency of Commitments with Privacy Policies and Procedures (1.2.5) | Internal personnel or advisers review contracts for consistency with privacy policies and procedures and address any inconsistencies.   | Accountability & Auditing | 2                   | Repeatable | Reviews of contracts for privacy considerations are incomplete and inconsistent.  | <b>Procedures exist to review contracts and other commitments for instances where personal information may be involved; however, such reviews are informal and not consistently used.</b>                    | A log of contracts exists and all contracts are reviewed for privacy considerations and concerns prior to execution.  | Existing contracts are reviewed upon renewal to ensure continued compliance with the privacy policies and procedures. Changes in the entity's privacy policies will trigger a review of existing contracts for compliance.        | Contracts are reviewed on a regular basis and tracked. An automated process has been set up to flag which contracts require immediate review when changes to privacy policies and procedures are implemented.   |

| GAPP Criteria                                  | Criteria Description  | CFPB Principle            | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined  | Managed   | Optimized   |  |
|--|---|---------------------------|---------------------|------------|---|--|---|---|--|
| Infrastructure and Systems Management (1.2.6)  | <p>The potential privacy impact is assessed when new processes involving personal information are implemented, and when changes are made to such processes (including any such activities outsourced to third parties or contractors), and personal information continues to be protected in accordance with the privacy policies. For this purpose, processes involving personal information include the design, acquisition, development, implementation, configuration, modification and management of the following:</p> <ul style="list-style-type: none"> <li>• Infrastructure Systems</li> <li>• Applications</li> <li>• Web sites</li> <li>• Procedures</li> <li>• Products and services</li> <li>• Data bases and information repositories</li> <li>• Mobile computing and other similar electronic devices</li> </ul> <p>The use of personal information in process and system test and development is prohibited unless such information is anonymized or otherwise protected in accordance with the entity's privacy policies and procedures.</p> | Accountability & Auditing | 2                   | Repeatable | Changes to existing processes or the implementation of new business and system processes for privacy issues is not consistently assessed. | Privacy impact is considered during changes to business processes and/or supporting application systems; however, these processes are not fully documented and the procedures are informal and inconsistently applied. | The entity has implemented formal procedures to assess the privacy impact of new and significantly changed products, services, business processes and infrastructure (sometimes referred to as a privacy impact assessment). The entity uses a documented systems development and change management process for all information systems and related technology employed to collect, use, retain, disclose and destroy personal information. | Management monitors and reviews compliance with policies and procedures that require a privacy impact assessment. | Through quality reviews and other independent assessments, management is informed of the effectiveness of the process for considering privacy requirements in all new and modified processes and systems. Such information is analyzed and, where necessary, changes made. |
| Privacy Incident and Breach Management (1.2.7) | A documented privacy incident and breach management program has been implemented that includes, but is not  | Accountability & Auditing | 2                   | Repeatable | Few procedures exist to identify and manage privacy incidents; however, they are not documented   | Procedures have been developed on how to deal with a privacy incident; however, they are   | A documented breach management plan has been implemented that includes: accountability, risk  | A walkthrough of the breach management plan is performed periodically and updates to the program are made as      | The internal and external privacy environments are monitored for issues affecting breach risk and breach response,   |

| GAPP Criteria | Criteria Description   | CFPB Principle | CFPB Maturity Level | Ad Hoc                          | Repeatable   | Defined   | Managed | Optimized  |
|---------------|--|----------------|---------------------|---------------------------------|--|---|---------|--|
|               | <p>limited to, the following:</p> <ul style="list-style-type: none"> <li>• Procedures for the identification, management and resolution of privacy incidents and breaches</li> <li>• Defined responsibilities</li> <li>• A process to identify incident severity and determine required actions and escalation procedures</li> <li>• A process for complying with breach laws and regulations, including stakeholder breach notification, if required</li> <li>• An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties or discipline, as appropriate</li> <li>• A process for periodic review (at least annually) of actual incidents to identify necessary program updates based on the following:                             <ul style="list-style-type: none"> <li>— Incident patterns and root cause</li> <li>—Changes in the internal control environment or external requirements (regulation or legislation)</li> </ul> </li> <li>• Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed</li> </ul> |                |                     | and are applied inconsistently. | not comprehensive and/or inadequate employee training has increased the likelihood of unstructured and inconsistent responses. | assessment, response, containment, communications (including possible notification to affected individuals and appropriate authorities, if required or deemed necessary), remediation (including post-breach analysis of the breach response) and resumption. | needed. | evaluated and improvements are made. Management assessments are provided after any privacy breach and analyzed; changes and improvements are made. |

| GAPP Criteria                                | Criteria Description  | CFPB Principle            | CFPB Maturity Level | Ad Hoc  | Repeatable   | Defined  | Managed   | Optimized   |  |
|--|---|---------------------------|---------------------|---------|--|--|---|---|--|
| Supporting Resources (1.2.8)                 | Resources are provided by the entity to implement and support its privacy policies.   | Accountability & Auditing | 3                   | Defined | Resources are only allocated on an "as needed" basis to address privacy issues as they arise.  | Privacy procedures exist; however, they have been "developed" within small units or groups without support from privacy specialists.   | Individuals with responsibility and/or accountability for privacy are empowered with authority and resources. Such resources are made available throughout the entity.  | Management ensures that adequately qualified privacy resources are identified and made available throughout the entity to support its various privacy initiatives.  | Management annually reviews its privacy program and seeks ways to improve the program's performance, including assessing the adequacy, availability and performance of resources.  |
| Qualifications of Internal Personnel (1.2.9) | The entity establishes qualifications for personnel responsible for protecting the privacy and security of personal information and assigns such responsibilities only to those personnel who meet these qualifications and have received the necessary training. | Accountability & Auditing | 4                   | Managed | The entity has not formally established qualifications for personnel who collect, use, disclose or otherwise handle personal information.          | The entity has some established qualifications for personnel who collect, disclose, use or otherwise handle personal information, but are not fully documented.<br><br>Employees receive some training on how to deal with personal information. | The entity defines qualifications for personnel who perform or manage the entity's collection, use and disclosure of personal information. Persons responsible for the protection and security of personal information have received appropriate training and have the necessary knowledge to manage the entity's collection, use and disclosure of personal information. | The entity has formed a nucleus of privacy qualified individuals to provide privacy support to assist with specific issues, including training and job assistance.  | The entity annually assesses the performance of their privacy program, including the performance and qualifications of their privacy-designated specialists. An analysis is performed of the results and changes or improvements made, as required.  |
| Privacy Awareness and Training (1.2.10)      | A privacy awareness program about the entity's privacy policies and related matters, and specific training for selected personnel depending on their roles and responsibilities, are provided.  | Awareness & Training      | 3                   | Defined | Formal privacy training is not provided to employees; however some knowledge of privacy may be obtained from other employees or anecdotal sources. | The entity has a privacy awareness program, but training is sporadic and inconsistent.   | Personnel who handle personal information have received appropriate privacy awareness and training to ensure the entity meets obligations in its privacy notice and applicable laws. Training is scheduled, timely and consistent.  | An enterprise-wide privacy awareness and training program exists and is monitored by management to ensure compliance with specific training requirements. The entity has determined which employees require privacy training and tracks their participation during such training. | A strong privacy culture exists. Compulsory privacy awareness and training is provided. Such training requires employees to complete assignments to validate their understanding. When privacy incidents or breaches occur, remedial training as well as changes to the training curriculum is made in a timely fashion. |

| GAPP Criteria  | Criteria Description   | CFPB Principle            | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined  | Managed  | Optimized   |  |
|--|--|---------------------------|---------------------|------------|--|--|--|---|--|
| Changes in Regulatory and Business Requirements (1.2.11) | For each jurisdiction in which the entity operates, the effect on privacy requirements from changes in the following factors is identified and addressed:<br>— Legal and regulatory<br>— Contracts, including service-level agreements<br>— Industry requirements<br>— Business operations and processes<br>— People, roles, and responsibilities<br>— Technology<br>Privacy policies and procedures are updated to reflect changes in requirements. | Accountability & Auditing | 2                   | Repeatable | Changes in business and regulatory environments are addressed sporadically in any privacy initiatives the entity may contemplate. Any privacy-related issues or concerns that are identified only occur in an informal manner. | The entity is aware that certain changes may impact their privacy initiatives; however, the process is not fully documented. | The entity has implemented policies and procedures designed to monitor and act upon changes in the business and/or regulatory environment. The procedures are inclusive and employees receive training in their use as part of an enterprise-wide privacy program. | The entity has established process to monitor the privacy environment and identify items that may impact its privacy program. Changes are considered in terms of the entity's legal, contracting, business, human resources and technology. | The entity has established a process to continually monitor and update any privacy obligations that may arise from changes to legislation, regulations, industry-specific requirements and business practices. |
| NOTICE (5 criteria)                                      | The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.   |                           |                     |            |  |  |  |   |  |
| Privacy Policies (2.1.0)                                 | The entity's privacy policies address providing notice to individuals.   | Openness & Transparency   | 2                   | Repeatable | Notice policies and procedures exist informally.   | Notice provisions exist in privacy policies and procedures but may not cover all aspects and are not fully documented.       | Notice provisions in privacy policies cover all relevant aspects and are fully documented.   | Compliance with notice provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.  | Management monitors compliance with privacy policies and procedures relating to notice. Issues of non-compliance are identified and remedial action taken to ensure compliance.                                |

| GAPP Criteria                           | Criteria Description   | CFPB Principle          | CFPB Maturity Level | Ad Hoc  | Repeatable   | Defined   | Managed  | Optimized  |
|---|--|-------------------------|---------------------|---|--|---|--|--|
| Communication to Individuals (2.1.1)    | <p>Notice is provided to individuals regarding the following privacy policies: purpose; choice/consent; collection; use/retention/disposal; access; disclosure to third parties; security for privacy; quality; and monitoring/enforcement.</p> <p>If personal information is collected from sources other than the individual, such sources are described in the notice.</p>                      | Openness & Transparency | 4 Managed           | Notice to individuals is not provided in a consistent manner and may not include all aspects of privacy, such as purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring/enforcement. | Notice is provided to individuals regarding some of the following privacy policies at or before the time of collection: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring / enforcement. | Notice is provided to individuals regarding all of the following privacy policies at or before collection and is documented: purpose; choice/consent; collection; use, retention and disposal; access; disclosure; security for privacy; quality; and monitoring / enforcement. | Privacy policies describe the consequences, if any, of not providing the requested information and indicate that certain information may be developed about individuals, such as buying patterns, or collected from other sources. | Changes and improvements to messaging and communications techniques are made in response to periodic assessments and feedback.   |
| Provision of Notice (2.2.1)             | <p>Notice is provided to the individual about the entity's privacy policies and procedures (a) at or before the time personal information is collected, or as soon as practical hereafter, (b) at or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, or (c) before personal information is used for new purposes not previously identified.</p> | Openness & Transparency | 3 Defined           | Notice may not be readily accessible nor provided on a timely basis.  | Notice provided to individuals is generally accessible but is not provided on a timely basis. Notice may not be provided in all cases when personal information is collected or used for new purposes.   | <b>The privacy notice is documented, readily accessible and available, provided in a timely fashion and clearly dated.</b>  | The entity tracks previous iterations of the privacy policies and individuals are informed about changes to a previously communicated privacy notice. The privacy notice is updated to reflect changes to policies and procedures. | The entity solicits input from relevant stakeholders regarding the appropriate means of providing notice and makes changes as deemed appropriate. Notice is provided using various techniques to meet the communications technologies of their constituents (e.g. social media, mobile communications, etc). |
| Entities and Activities Covered (2.2.2) | <p>An objective description of the entities and activities covered by privacy policies is included in the privacy notice.</p>  | Openness & Transparency | 3 Defined           | The privacy notice may not include all relevant entities and activities.  | The privacy notice describes some of the particular entities, business segments, locations, and types of information covered.  | <b>The privacy notice objectively describes and encompasses all relevant entities, business segments, locations, and types of information covered.</b>  | The entity performs a periodic review to ensure the entities and activities covered by privacy policies are updated and accurate.  | Management follows a formal documented process to consider and take appropriate action as necessary to update privacy policies and the privacy notice prior to any change in the entity's business structure and activities.   |

| GAPP Criteria                          | Criteria Description  | CFPB Principle                            | CFPB Maturity Level | Ad Hoc  | Repeatable  | Defined   | Managed   | Optimized   |
|--|---|---|---------------------|---|---|---|---|---|
| Clear and Conspicuous (2.2.3)          | The privacy notice is conspicuous and uses clear language.  | Openness & Transparency                   | 2 Repeatable        | Privacy policies are informal, not documented and may be phrased differently when orally communicated.                                | The privacy notice may be informally provided but is not easily understood, nor is it easy to see or easily available at points if data collection. If a formal privacy notice exists, it may not be clear and conspicuous.   | The privacy notice is in plain and simple language, appropriately labeled, easy to see, and not in small print. Privacy notices provided electronically are easy to access and navigate.  | Similar formats are used for different and relevant subsidiaries or segments of an entity to avoid confusion and allow consumers to identify any differences. Notice formats are periodically reviewed for clarity and consistency.                           | Feedback about improvements to the readability and content of the privacy policies are analyzed and incorporated into future versions of the privacy notice.                                |
| <b>CHOICE and CONSENT (7 criteria)</b> | <b>The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.</b>   |   |                     |   |   |   |   |   |
| Privacy Policies (3.1.0)               | The entity's privacy policies address the choices to individuals and the consent to be obtained.  | Limits on uses and sharing of information | 2 Repeatable        | Choice and consent policies and procedures exist informally.  | Choice and consent provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.   | Choice and consent provisions in privacy policies and procedures cover all relevant aspects and are fully documented.   | Compliance with choice and consent provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.  | Management monitors compliance with privacy policies and procedures relating to choice and consent. Issues of non-compliance are identified and remedial action taken to ensure compliance. |
| Communication to Individuals (3.1.1)   | Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise. | Limits on uses and sharing of information | 3 Defined           | Individuals may be informed about the choices available to them; however, communications are inconsistent, sporadic and undocumented. | The entity's privacy notice describes in a clear and concise manner some of the following: 1) choices available to the individual regarding collection, use, and disclosure of personal information, 2) the process an individual should follow to exercise these choices, 3) the ability of, and process for, an individual to change contact preferences and 4) the consequences of failing to provide personal information required. | <b>The entity's privacy notice describes, in a clear and concise manner, all of the following: 1) choices available to the individual regarding collection, use, and disclosure of personal information, 2) the process an individual should follow to exercise these choices, 3) the ability of, and process for, an individual to change contact preferences and 4) the consequences of failing to provide personal information required.</b> | Privacy policies and procedures are reviewed periodically to ensure the choices available to individuals are updated as necessary and the use of explicit or implicit consent is appropriate with regard to the personal information being used or disclosed. | Changes and improvements to messaging and communications techniques and technologies are made in response to periodic assessments and feedback.   |

| GAPP Criteria  | Criteria Description  | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined  | Managed   | Optimized  |  |
|--|---|---|---------------------|------------|---|--|---|--|--|
| Consequences of Denying or Withdrawing Consent (3.1.2) | When personal information is collected, individuals are informed of the consequences of refusing to provide personal information or of denying or withdrawing consent to use personal information for purposes identified in the notice.                          | Openness & Transparency                   | 3                   | Defined    | Individuals may not be informed consistently about the consequences of refusing, denying or withdrawing.        | Consequences may be identified but may not be fully documented or consistently disclosed to individuals.   | Individuals are informed about the consequences of refusing to provide personal information or denying withdrawing consent.   | Processes are in place to review the stated consequences periodically to ensure completeness, accuracy and relevance.  | Processes are implemented to reduce the consequences of denying consent, such as increasing the granularity of the application of such consequences.   |
| Implicit or Explicit Consent (3.2.1)                   | Implicit or explicit consent is obtained from the individual at or before the time personal information is collected or soon after. The individual's preferences expressed in his or her consent are confirmed and implemented.                                   | Limits on uses and sharing of information | 3                   | Defined    | Consent is neither documented nor consistently obtained at or before collection of personal information.        | Consent is consistently obtained, but may not be documented or obtained in a timely fashion.   | Consent is obtained before or at the time personal information is collected and preferences are implemented (such as making appropriate database changes and ensuring that access the database test for the preference). Explicit consent is documented and implicit consent processes are appropriate. Processes are in place to ensure that consent is recorded by the entity and referenced prior to future use. | An individual's preferences are confirmed and any changes are documented and referenced prior to future use.   | Consent processes are periodically reviewed to ensure the individual's preferences are being appropriately recorded and acted upon and, where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information. |
| Consent for New Purposes and Uses (3.2.2)              | If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and implicit or explicit consent is obtained prior to such new use or purpose. | Limits on uses and sharing of information | 2                   | Repeatable | Individuals are not consistently notified about new proposed uses of personal information previously collected. | Individuals are consistently notified about new purposes not previously specified. A process exists to notify individuals but may not be fully documented and consent might not be obtained before new uses. | Consent is obtained and documented prior to using personal information for purposes other than those for which it was originally collected.   | Processes are in place to ensure personal information is used only in accordance with the purposes for which consent has been obtained and to ensure it is not used if consent is withdrawn. Monitoring is in place to ensure personal information is not used without proper consent. | Consent processes are periodically reviewed to ensure consent for new purposes is being appropriately recorded and acted upon and where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information.       |

| GAPP Criteria   | Criteria Description  | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined   | Managed   | Optimized   |   |
|---|---|---|---------------------|------------|---|---|---|---|---|
| Explicit Consent for Sensitive Information (3.2.3)  | Explicit consent is obtained directly from the individual when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise. | Limits on uses and sharing of information | 3                   | Defined    | Explicit consent is not consistently obtained prior to collection of sensitive personal information.  | Employees who collect personal information are aware that explicit consent is required when obtaining sensitive personal information; however, the process is not well defined or fully documented. | <b>A documented formal process has been implemented requiring explicit consent be obtained directly from the individual prior to, or as soon as practically possible, after collection of sensitive personal information.</b>   | The process is reviewed and compliance monitored to ensure explicit consent is obtained prior to, or as soon as practically possible, after collection of sensitive personal information. | For procedures that collect sensitive personal information and do not obtain explicit consent, remediation plans are identified and implemented to ensure explicit consent has been obtained.                           |
| Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices (3.2.4) | Consent is obtained before personal information is transferred to/from an individual's computer or similar device.  | Limits on uses and sharing of information | 2                   | Repeatable | Consent is not consistently obtained before personal information is transferred to/from another computer or other similar device.   | <b>Software enables an individual to provide consent before personal information is transferred to/from another computer or other similar device.</b>   | The application is designed to consistently solicit and obtain consent before personal information is transferred to/from another computer or other similar device and does not make any such transfers if consent has not been obtained. Such consent is documented. | The process is reviewed and compliance monitored to ensure consent is obtained before any personal information is transferred to/from an individual's computer or other similar device.   | Where procedures have been identified that do not obtain consent before personal information is transferred to/from an individual's computer or other similar device, remediation plans are identified and implemented. |
| <b>COLLECTION (7 criteria)</b>  | <b>The entity collects personal information only for the purposes identified in the notice.</b>   |   |                     |            |   |   |   |   |   |
| Privacy Policies (4.1.0)  | The entity's privacy policies address the collection of personal information.   | Purpose of collection                     | 2                   | Repeatable | Collection policies and procedures exist informally.  | <b>Collection provisions in privacy policies exist but might not cover all aspects, and are not fully documented.</b>   | Collection provisions in privacy policies cover all relevant aspects of collection and are fully documented.  | Compliance with collection provisions in privacy policies and procedures is monitored and the results of such monitoring are used to reinforce key privacy messages.                      | Management monitors compliance with privacy policies and procedures relating to collection. Issues of non-compliance are identified and remedial action taken to ensure compliance.                                     |
| Communication to Individuals (4.1.1)  | Individuals are informed that personal information is collected only for the purposes identified in the notice.   | Purpose of collection                     | 3                   | Defined    | Individuals may be informed that personal information is collected only for purposes identified in the notice; however, communications are inconsistent, sporadic and undocumented. | Individuals are informed that personal information is collected only for the purposes identified in the notice. Such notification is generally not documented.                                      | <b>Individuals are informed that personal information is collected only for the purposes identified in the notice and the sources and methods used to collect this personal information are identified. Such notification is available in written format.</b>         | Privacy policies are reviewed periodically to ensure the areas related to collection are updated as necessary.  | Changes and improvements to messaging and communications methods and techniques are made in response to periodic assessments and feedback.  |

| GAPP Criteria   | Criteria Description  | CFPB Principle          | CFPB Maturity Level | Ad Hoc   | Repeatable  | Defined  | Managed  | Optimized   |
|---|---|-------------------------|---------------------|--|---|--|--|---|
| Types of Personal Information Collected and Methods of Collection (4.1.2) | The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are documented and described in the privacy notice. | Openness & Transparency | 3<br>Defined        | Individuals may be informed about the types of personal information collected and the methods of collection; however, communications are informal, may not be complete and may not fully describe the methods of collection. | The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are neither fully documented nor fully described in the privacy notice.   | The types of personal information collected and the methods of collection, including the use of cookies or other tracking techniques, are fully documented and fully described in the privacy notice.<br><br>The notice also discloses whether information is developed or acquired about individuals, such as buying patterns. The notice also describes the consequences if the cookie is refused. | Management monitors business processes to identify new types of personal information collected and new methods of collection to ensure they are described in the privacy notice. | The privacy notice is reviewed regularly and updated in a timely fashion to describe all the types of personal information being collected and the methods used to collect them.  |
| Collection Limited to Identified Purpose (4.2.1)                          | The collection of personal information is limited to that necessary for the purposes identified in the notice.  | Data minimization       | 2<br>Repeatable     | Informal and undocumented procedures are relied upon to ensure collection is limited to that necessary for the purposes identified in the privacy notice.  | Policies and procedures, may not:<br><ul style="list-style-type: none"> <li>• be fully documented;</li> <li>• distinguish the personal information essential for the purposes identified in the notice;</li> <li>• differentiate personal information from optional information.</li> </ul> | Policies and procedures that have been implemented are fully documented to clearly distinguish the personal information essential for the purposes identified in the notice and differentiate it from optional information. Collection of personal information is limited to information necessary for the purposes identified in the privacy notice.  | Policies and procedures are in place to periodically review the entity's needs for personal information.   | Policies, procedures and business processes are updated due to changes in the entity's needs for personal information. Corrective action is undertaken when information not necessary for the purposes identified is collected. |

| GAPP Criteria                                   | Criteria Description   | CFPB Principle             | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined   | Managed  | Optimized  |  |
|---|--|----------------------------|---------------------|------------|---|---|--|--|--|
| Collection by Fair and Lawful Means (4.2.2)     | Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information. | Accountability & Auditing  | 2                   | Repeatable | Informal procedures exist limiting the collection of personal information to that which is fair and lawful; however, they may be incomplete and inconsistently applied. | Management may conduct reviews of how personal information is collected, but such reviews are inconsistent and untimely. Policies and procedures related to the collection of personal information are either not fully documented or incomplete. | Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information. | Methods of collecting personal information are periodically reviewed by management after implementation to confirm personal information is obtained fairly and lawfully.   | Complaints to the entity are reviewed to identify where unlawful or deceptive practices exist. Such complaints are reviewed, analyzed and changes to policies and procedures to correct such practices are implemented.              |
| Collection from Third Parties (4.2.3)           | Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.   | Data quality and integrity | 2                   | Repeatable | Limited guidance and direction exist to assist in the review of third-party practices regarding collection of personal information.                                     | Reviews of third party practices are performed but such procedures are not fully documented.  | The entity consistently reviews privacy policies, collection methods, and types of consents of third parties before accepting personal information from third-party data sources. Clauses are included in agreements that require third-parties to collect information fairly and lawfully and in accordance with the entity's privacy policies.           | Once agreements have been implemented, the entity conducts a periodic review of third-party collection of personal information. Corrective actions are discussed with third parties.   | Lessons learned from contracting and contract management processes are analyzed and, where appropriate, improvements are made to existing and future contracts involving collection of personal information involving third parties. |
| Information Developed About Individuals (4.2.4) | Individuals are informed if the entity develops or acquires additional information about them for its use.   | Openness & Transparency    | 3                   | Defined    | Policies and procedures informing individuals that additional information about them is being collected or used are informal, inconsistent and incomplete.              | Policies and procedures exist to inform individuals when the entity develops or acquires additional personal information about them for its use; however, procedures are not fully documented or consistently applied.                            | The entity's privacy notice indicates that, if applicable, it may develop and/or acquire information about individuals by using third-party sources, browsing, e-mail content, credit and purchasing history. Additional consent is obtained where necessary.  | The entity monitors information collection processes, including the collection of additional information, to ensure appropriate notification and consent requirements are complied with. Where necessary, changes are implemented. | The entity's privacy notice provides transparency in the collection, use and disclosure of personal information. Individuals are given multiple opportunities to learn how personal information is developed or acquired.            |

| GAPP Criteria                                   | Criteria Description  | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined   | Managed  | Optimized   |  |
|---|---|---|---------------------|------------|--|---|--|---|--|
| <b>USE, RETENTION AND DISPOSAL (5 criteria)</b> | The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.   |   |                     |            |  |   |  |   |  |
| <b>Privacy Policies (5.1.0)</b>                 | The entity's privacy policies address the use, retention, and disposal of personal information.   | Limits on uses and sharing of information | 2                   | Repeatable | Procedures for the use, retention and disposal of personal information are ad hoc, informal and likely incomplete.   | Use, retention and disposal provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.  | Use, retention and disposal provisions in privacy policies and procedures cover all relevant aspects and are fully documented.   | Compliance with use, retention and disposal provisions in privacy policies and procedures is monitored.                   | Management monitors compliance with privacy policies and procedures relating to use, retention and disposal. Issues of non-compliance are identified and remedial action taken to ensure compliance in a timely fashion. |
| <b>Communication to Individuals (5.1.1)</b>     | Individuals are informed that personal information is (a) used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise, (b) retained for no longer than necessary to fulfill the stated purposes, or for a period specifically required by law or regulation, and (c) disposed of in a manner that prevents loss, theft, misuse or unauthorized access. | Limits on uses and sharing of information | 3                   | Defined    | Individuals may be informed about the uses, retention and disposal of their personal information; however, communications are inconsistent, sporadic and undocumented. | Individuals are informed about the use, retention and disposal of personal information, but this communication may not cover all aspects and is not fully documented. Retention periods are not uniformly communicated. | Individuals are consistently and uniformly informed about use, retention and disposal of personal information.<br><br>Data retention periods are identified and communicated to individuals. | Methods are in place to update communications to individuals when changes occur to use, retention and disposal practices. | Individuals' general level of understanding of use, retention and disposal of personal information is assessed. Feedback is used to continuously improve communication methods.  |

| GAPP Criteria   | Criteria Description  | CFPB Principle        | CFPB Maturity Level | Ad Hoc  | Repeatable   | Defined  | Managed  | Optimized  |   |
|---|---|-----------------------|---------------------|---------|--|--|--|--|---|
| Use of Personal Information (5.2.1)                                 | Personal information is used only for the purposes identified in the notice and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise. | Purpose of collection | 3                   | Defined | The use of personal information may be inconsistent with the purposes identified in the notice. Consent is not always obtained consistently. | Policies and procedures regarding the use of information have been adopted; however, they are not documented and may not be consistently applied.  | Use of personal information is consistent with the purposes identified in the privacy notice. Consent for these uses is consistently obtained. Uses of personal information throughout the entity are in accordance with the individual's preferences and consent. | Uses of personal information are monitored and periodically reviewed for appropriateness. Management ensures that any discrepancies are corrected on a timely basis.     | The uses of personal information are monitored and periodically assessed for appropriateness; verifications of consent and usage are conducted through the use of automation. Any discrepancies are remediated in a timely fashion. Changes to laws and regulations are monitored and the entity's policies and procedures are amended as required. |
| Retention of Personal Information (5.2.2)                           | Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.  | Data minimization     | 3                   | Defined | The retention of personal information is irregular and inconsistent.   | Policies and procedures for identifying retention periods of personal information have been adopted, but may not be fully documented or cover all relevant aspects.  | The entity has documented its retention policies and procedures and consistently retains personal information in accordance with such policies and practices.  | Retention practices are periodically reviewed for compliance with policies and changes implemented when necessary.   | The retention of personal information is monitored and periodically assessed for appropriateness, and verifications of retention are conducted. Such processes are automated to the extent possible.<br><br>Any discrepancies found are remediated in a timely fashion.   |
| Disposal, Destruction and Redaction of Personal Information (5.2.3) | Personal information no longer retained is anonymized, disposed of or destroyed in a manner that prevents loss, theft, misuse or unauthorized access.   | Data minimization     | 3                   | Defined | The disposal, destruction and redaction of personal information is irregular, inconsistent and incomplete.                                   | Policies and procedures for identifying appropriate and current processes and techniques for the appropriate disposal, destruction and redaction of personal information have been adopted but are not fully documented or complete. | The entity has documented its policies and procedures regarding the disposal, destruction and redaction of personal information, implemented such practices and ensures that these practices are consistent with the privacy notice.                               | The disposal, destruction, and redaction of personal information are consistently documented and periodically reviewed for compliance with policies and appropriateness. | The disposal, destruction, and redaction of personal information are monitored and periodically assessed for appropriateness, and verification of the disposal, destruction and redaction conducted. Such processes are automated to the extent possible.<br><br>Any discrepancies found are remediated in a timely fashion.                        |
| ACCESS (8 criteria)   | The entity provides individuals with access to their personal information for review and update.  |                       |                     |         |  |  |  |  |   |

| GAPP Criteria                        | Criteria Description  | CFPB Principle           | CFPB Maturity Level | Ad Hoc   | Repeatable   | Defined  | Managed   | Optimized  |
|--------------------------------------|---|--------------------------|---------------------|--|--|--|---|--|
| Privacy Policies (6.1.0)             | The entity's privacy policies address providing individuals with access to their personal information.                                  | Individual participation | 4<br>Managed        | Informal access policies and procedures exist.   | Access provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.  | Access provisions in privacy policies and procedures exist—but may not cover all aspects, and are not fully documented.  | Compliance with access provisions in privacy policies and procedures is monitored.  | Management monitors compliance with privacy policies and procedures relating to access. Issues of non-compliance are identified and remedial action taken to ensure compliance.  |
| Communication to Individuals (6.1.1) | Individuals are informed about how they may obtain access to their personal information to review, update and correct that information. | Individual participation | 3<br>Defined        | Individuals may be informed about how they may obtain access to their personal information; however, communications are inconsistent, sporadic and undocumented. | Individuals are usually informed about procedures available to them to access their personal information, but this communication process may not cover all aspects and is not fully documented. Update and correction options may not be uniformly communicated. | Individuals are consistently and uniformly informed about procedures available to them to access their personal information held by the entity. Personal information update and correction options are identified and communicated to individuals. | Processes are in place to update communications to individuals when changes occur to access policies, procedures and practices. | The entity ensures that individuals are informed about their personal information access rights, including update and correction options, through channels such as direct communication programs, notification on statements and other mailings and training and awareness programs for staff. Management monitors and assesses the effects of its various initiatives and seeks to continuously improve methods of communication and understanding. |

| GAPP Criteria   | Criteria Description   | CFPB Principle           | CFPB Maturity Level | Ad Hoc  | Repeatable  | Defined  | Managed  | Optimized   |   |
|---|--|--------------------------|---------------------|---------|---|--|--|---|---|
| Access by Individuals to their Personal Information (6.2.1) | Individuals are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information. | Individual participation | 4                   | Managed | The entity has informal procedures granting individuals access to their information; however, such procedures are not documented and may not be consistently applied. | Some procedures are in place to allow individuals to access their personal information, but they may not cover all aspects and may not be fully documented.  | Procedures to search for an individual's personal information and to grant individuals access to their information have been documented, implemented and cover all relevant aspects. Employees have been trained in how to respond to these requests, including recording such requests. | Procedures are in place to ensure individuals receive timely communication of what information the entity maintains about them and how they can obtain access. The entity monitors information and access requests to ensure appropriate access to such personal information is provided. The entity identifies and implements measures to improve the efficiency of its searches for an individual's personal information. | The entity reviews the processes used to handle access requests to determine where improvements may be made and implements such improvements. Access to personal information is automated and self service when possible and appropriate.   |
| Confirmation of an Individual's Identity (6.2.2)            | The identity of individuals who request access to their personal information is authenticated before they are given access to that information.                    | Individual participation | 4                   | Managed | Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.                            | Procedures are in place to confirm the identity of individuals requesting access to their personal information before they are granted access, but do not cover all aspects and may not be documented. Level of authentication required may not be appropriate to the personal information being accessed. | Confirmation/authentication methods have been implemented to uniformly and consistently confirm the identity of individuals requesting access to their personal information, including the training of employees.  | Procedures are in place to track and monitor the confirmation/authentication of individuals before they are granted access to personal information, and to review the validity of granting access to such personal information.   | The successful confirmation/authentication of individuals before they are granted access to personal information is monitored and periodically assessed for type 1 (where errors are not caught) and type 2 (where an error has been incorrectly identified) errors. Remediation plans to lower the error rates are formulated and implemented. |

| GAPP Criteria   | Criteria Description  | CFPB Principle           | CFPB Maturity Level | Ad Hoc   | Repeatable   | Defined  | Managed  | Optimized  |
|---|---|--------------------------|---------------------|--|--|--|--|--|
| Understandable Personal Information, Time Frame, and Cost (6.2.3) | Personal information is provided to the individual in an understandable form, in a reasonable timeframe, and at a reasonable cost, if any.  | Individual participation | 4 Managed           | The entity has some informal procedures designed to provide information to individuals in an understandable form. Timeframes and costs charged may be inconsistent and unreasonable.     | Procedures are in place requiring that personal information be provided to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost, but may not be fully documented or cover all aspects.   | Procedures have been implemented that consistently and uniformly provide personal information to the individual in an understandable form, in a reasonable timeframe and at a reasonable cost.   | Procedures are in place to track and monitor the response time in providing personal information, the associated costs incurred by the entity and any charges to the individual making the request. Periodic assessments of the understandability of the format for information provided to individuals are conducted. | Reports of response times in providing personal information are monitored and assessed. The associated costs incurred by the entity and any charges to the individual making the request are periodically assessed. Periodic assessments of the understandability of the format for information provided to individuals are conducted. Remediation plans are made and implemented for unacceptable response time, excessive or inconsistent charges and difficult-to-read personal information report formats. Conversion of personal information to an understandable form is automated where possible and appropriate. |
| Denial of Access (6.2.4)  | Individuals are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation. | Individual participation | 4 Managed           | Informal procedures are used to inform individuals, of the reason a request for access to their personal information was denied; however they are incomplete and inconsistently applied. | Procedures are in place to inform individuals of the reason a request for access to their personal information was denied, but they may not be documented or cover all aspects. Notification may not be in writing or include the entity's legal rights to deny such access and the individual's right to challenge denials. | Consistently applied and uniform procedures have been implemented to inform individuals in writing of the reason a request for access to their personal information was denied. The entity's legal rights to deny such access have been identified as well as the individual's right to challenge denials. | Procedures are in place to review the response time to individuals whose access request has been denied, reasons for such denials, as well as any communications regarding challenges.   | Reports of denial reasons, response times and challenge communications are monitored and assessed. Remediation plans are identified and implemented for unacceptable response time and inappropriate denials of access.<br><br>The denial process is automated and includes electronic responses where possible and appropriate.   |

| GAPP Criteria                                       | Criteria Description   | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined  | Managed  | Optimized  |   |
|---|--|---|---------------------|------------|--|--|--|--|---|
| Updating or Correcting Personal Information (6.2.5) | Individuals are able to update or correct personal information held by the entity. If practical and economically feasible to do so, the entity provides such updated or corrected information to third parties that previously were provided with the individual's personal information. | Individual participation                  | 3                   | Defined    | Informal and undocumented procedures exist that provide individuals with information on how to update or correct personal information held by the entity; however, they are incomplete and inconsistently applied. | Some procedures are in place for individuals to update or correct personal information held by the entity, but they are not complete and may not be fully documented. A process exists to review and confirm the validity of such requests and inform third parties of changes made; however, not all of the processes are documented. | Documented policies with supporting procedures have been implemented to consistently and uniformly inform individuals of how to update or correct personal information held by the entity. Procedures have been implemented to consistently and uniformly provide updated information to third parties that previously received the individual's personal information. | Procedures are in place to track data update and correction requests and to validate the accuracy and completeness of such data. Documentation or justification is kept for not providing information updates to relevant third parties. | Reports of updates and correction requests and response time to update records are monitored and assessed. Documentation or justification for not providing information updates to relevant third parties is monitored and assessed to determine whether the economically feasible requirement was met. Updating is automated and self-service where possible and appropriate. Distribution of updated information to third parties is also automated where possible and appropriate. |
| Statement of Disagreement (6.2.6)                   | Individuals are informed, in writing, about the reason a request for correction of personal information was denied, and how they may appeal.   | Individual participation                  | 3                   | Defined    | Procedures used to inform individuals of the reason a request for correction of personal information was denied, and how they may appeal are inconsistent and undocumented.  | Procedures are in place to inform individuals about the reason a request for correction of personal information was denied, and how they may appeal, but they are not complete or documented.  | Documented policies and procedures that cover relevant aspects have been implemented to inform individuals in writing about the reason a request for correction of personal information was denied, and how they may appeal.   | Procedures are in place to track and review the reasons a request for correction of personal information was denied.   | Cases that involve disagreements over the accuracy and completeness of personal information are reviewed and remediation plans are identified and implemented as appropriate. The process to complete a Statement of Disagreement is automated where possible and appropriate.  |
| DISCLOSURE TO THIRD PARTIES (7 criteria)            | The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.   |   |                     |            |  |  |  |  |   |
| Privacy Policies (7.1.0)                            | The entity's privacy policies address the disclosure of personal information to third parties.   | Limits on uses and sharing of information | 2                   | Repeatable | Informal disclosure policies and procedures exist but may not be consistently applied.   | Disclosure provisions in privacy policies exist but may not cover all aspects, and are not fully documented.   | Disclosure provisions in privacy policies cover all relevant aspects and are fully documented.   | Compliance with disclosure provisions in privacy policies is monitored.  | Management monitors compliance with privacy policies and procedures relating to disclosure to third parties. Issues of non-compliance are identified and remedial action taken to ensure compliance.  |

| GAPP Criteria                          | Criteria Description   | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined  | Managed   | Optimized   |   |
|--|--|---|---------------------|------------|--|--|---|---|---|
| Communication to Individuals (7.1.1)   | Individuals are informed that personal information is disclosed to third parties only for the purposes identified in the notice and for which the individual has provided implicit or explicit consent unless a law or regulation specifically allows or requires otherwise. | Limits on uses and sharing of information | 2                   | Repeatable | Individuals may be informed that personal information is disclosed to third parties only for the purposes identified in the notice; however, communications are inconsistent, sporadic and undocumented. | Procedures are in place to inform individuals that personal information is disclosed to third parties; however, limited documentation exists and the procedures may not be performed consistently or in accordance with relevant laws and regulations. | Documented procedures that cover all relevant aspects, and in accordance with relevant laws and regulations are in place to inform individuals that personal information is disclosed to third parties, but only for the purposes identified in the privacy notice and for which the individual has provided consent. Third parties or classes of third parties to whom personal information is disclosed are identified. | Procedures exist to review new or changed business processes, third parties or regulatory bodies requiring compliance to ensure appropriate communications to individuals are provided and consent obtained where necessary.                                    | Issues identified or communicated to the entity with respect to the disclosure of personal information to third parties are monitored and, where necessary, changes and improvements made to the policies and procedures to better inform individuals.            |
| Communication to Third Parties (7.1.2) | Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.   | Limits on uses and sharing of information | 2                   | Repeatable | Procedures to communicate to third parties their responsibilities with respect to personal information provided to them are informal, inconsistent and incomplete.                                       | Procedures are in place to communicate to third parties the entity's privacy policies or other specific instructions or requirements for handling personal information, but they are inconsistently applied and not fully documented.                  | Documented policies and procedures exist and are consistently and uniformly applied to communicate to third parties the privacy policies or other specific instructions or requirements for handling personal information. Written agreements with third parties are in place confirming their adherence to the entity's privacy policies and procedures.   | A review is periodically performed to ensure third parties have received the entity's privacy policies, instructions and other requirements relating to personal information that has been disclosed. Acknowledgement of the receipt of the above is monitored. | Contracts and other agreements involving personal information provided to third parties are reviewed to ensure the appropriate information has been communicated and agreement has been obtained. Remediation plans are developed and implemented where required. |

| GAPP Criteria                              | Criteria Description  | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined   | Managed  | Optimized   |   |
|--|---|---|---------------------|------------|---|---|--|---|---|
| Disclosure of Personal Information (7.2.1) | Personal information is disclosed to third parties only for the purposes described in the notice, and for which the individual has provided implicit or explicit consent, unless a law or regulation specifically requires or allows otherwise. | Limits on uses and sharing of information | 2                   | Repeatable | Procedures regarding the disclosure of personal information to third parties are informal, incomplete and applied inconsistently. | Procedures are in place to ensure disclosure of personal information to third parties is only for the purposes described in the privacy notice and for which the individual has provided consent, unless laws or regulations allow otherwise; however, such procedures may not be fully documented or consistently and uniformly evaluated. | Documented procedures covering all relevant aspects have been implemented to ensure disclosure of personal information to third parties is only for the purposes described in the privacy notice and for which the individual has provided consent, unless laws or regulations allow otherwise. They are uniformly and consistently applied. | Procedures are in place to test and review whether disclosure to third parties is in compliance with the entity's privacy policies. | Reports of personal information provided to third parties are maintained and such reports are reviewed to ensure only information that has consent has been provided to third parties. Remediation plans are developed and implemented where inappropriate disclosure has occurred or where third parties are not in compliance with their commitments. Disclosure to third parties may be automated. |

| GAPP Criteria                              | Criteria Description   | CFPB Principle                            | CFPB Maturity Level | Ad Hoc   | Repeatable  | Defined   | Managed  | Optimized  |
|--|--|---|---------------------|--|---|---|--|--|
| Protection of Personal Information (7.2.2) | Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements. | Limits on uses and sharing of information | 2 Repeatable        | Procedures used to ensure third-party agreements are in place to protect personal information prior to disclosing to third parties are informal, incomplete and inconsistently applied. The entity does not have procedures to evaluate the effectiveness of third-party controls to protect personal information. | Procedures are in place to ensure personal information is disclosed only to third parties that have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements, but are not consistently and uniformly applied or fully documented. Some procedures are in place to determine whether third parties have reasonable controls; however, they are not consistently and uniformly assessed. | Documented policies and procedures covering all relevant aspects have been implemented to ensure personal information is disclosed only to third parties that have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy policies or other specific instructions or requirements. The entity has procedures to evaluate whether third parties have effective controls to meet the terms of the agreement, instructions or requirements. | An assessment of third party procedures is periodically performed to ensure such procedures continue to meet the entity's requirements. Such assessments may be performed by the entity or an independent qualified third party. | Changes in a third party environment are monitored to ensure the third party can continue to meet its obligations with respect to personal information disclosed to them. Remediation plans are developed and implemented where necessary. The entity evaluates compliance using a number of approaches to obtain an increasing level of assurance depending on its risk assessment. |

| GAPP Criteria   | Criteria Description   | CFPB Principle                            | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined   | Managed  | Optimized   |   |
|---|--|---|---------------------|------------|---|---|--|---|---|
| New Purposes and Uses (7.2.3)                           | Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of the individual.      | Limits on uses and sharing of information | 2                   | Repeatable | Procedures to ensure the proper disclosure of personal information to third parties for new purposes or uses are informal, inconsistent and incomplete. | Procedures exist to ensure the proper disclosure of personal information to third parties for new purposes; however, they may not be consistently and uniformly applied and not fully documented. | Documented procedures covering all relevant aspects have been implemented to ensure the proper disclosure of personal information to third parties for new purposes. Such procedures are uniformly and consistently applied. Consent from individuals prior to disclosure is documented. Existing agreements with third parties are reviewed and updated to reflect the new purposes and uses. | Monitoring procedures are in place to ensure proper disclosure of personal information to third parties. The entity monitors to ensure the newly disclosed information is only being used for the new purposes or as specified. | Reports of disclosure of personal information to third parties for new purposes and uses, as well as the associated consent by the individual, where applicable, are monitored and assessed, to ensure appropriate consent has been obtained and documented. Collection of consent for new purposes and uses is automated where possible and appropriate. |
| Misuse of Personal Information by a Third Party (7.2.4) | The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information. | Limits on uses and sharing of information | 2                   | Repeatable | Procedures to determine and address misuse of personal information by a third party are informal, incomplete and inconsistently applied.                | Procedures are in place to require remedial action in response to misuse of personal information by a third party, but they are not consistently and uniformly applied or fully documented.       | Documented policies and procedures covering all relevant aspects are in place to take remedial action in response to misuse of personal information by a third party. Such procedures are consistently and uniformly applied.  | Monitoring procedures are in place to track the response to misuse of personal information by a third party from initial discovery through to remedial action.  | Exception reports are used to record inappropriate or unacceptable activities by third parties and to monitor the status of remedial activities.<br><br>Remediation plans are developed and procedures implemented to address unacceptable or inappropriate use.  |
| <b>SECURITY FOR PRIVACY (9 criteria)</b>                | <b>The entity protects personal information against unauthorized access (both physical and logical).</b>   |   |                     |            |   |   |  |   |   |
| Privacy Policies (8.1.0)                                | The entity's privacy policies (including any relevant security policies) address the security of personal information.                               | Security                                  | 2                   | Repeatable | Security policies and procedures exist informally; however, they are based on ad hoc and inconsistent processes.  | Security provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.   | Security provisions in privacy policies cover all relevant aspects and are fully documented.   | Compliance with security provisions in privacy policies and procedures is evaluated and monitored.  | Management monitors compliance with privacy policies and procedures relating to security. Issues of non-compliance are identified and remedial action taken to ensure compliance.   |

| GAPP Criteria                        | Criteria Description   | CFPB Principle          | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined  | Managed   | Optimized  |  |
|--------------------------------------|--|-------------------------|---------------------|------------|--|--|---|--|--|
| Communication to Individuals (8.1.1) | Individuals are informed that precautions are taken to protect personal information.   | Openness & Transparency | 2                   | Repeatable | Individuals may be informed about security of personal information; however, communications are inconsistent, sporadic and undocumented. | Individuals are informed about the entity's security practices for the protection of personal information. Security policies, procedures and practices are documented and implemented. | The entity manages its security program through periodic reviews and security assessments. Incidents and violations of its communications policy for security are investigated.   | Communications explain to individuals the need for security, the initiatives the entity takes to ensure that personal information is protected and informs individuals of other activities they may want to take to further protect their information. |  |
| Information Security Program (8.2.1) | A security program has been developed, documented, approved, and implemented that includes administrative, technical and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the security of personal information:<br>a. Risk assessment and treatment [1.2.4]<br>b. Security policy [8.1.0]<br>c. Organization of information security [sections 1, 7, and 10]<br>d. Asset management [section 1]<br>e. Human resources security [section 1]<br>f. Physical and environmental security [8.2.3 and 8.2.4]<br>g. Communications and operations management [sections 1, 7, and 10]<br>h. Access control [sections 1,8.2, and 10]<br>i. Information systems acquisition, development, and | Security                | 2                   | Repeatable | There have been some thoughts of a privacy- focused security program, but limited in scope and perhaps undocumented.                     | The entity has a security program in place that may not address all areas or be fully documented.  | The entity has developed, documented and promulgated its comprehensive enterprise-wide security program. The entity has addressed specific privacy-focused security requirements. | Management monitors weaknesses, periodically reviews its security program as it applies to personal information and establishes performance benchmarks.  | The entity undertakes annual reviews of its security program, including external reviews, and determines the effectiveness of its procedures. The results of such reviews are used to update and improve the security program. |

| GAPP Criteria                   | Criteria Description  | CFPB Principle | CFPB Maturity Level | Ad Hoc  | Repeatable  | Defined  | Managed  | Optimized   |  |
|---------------------------------|---|----------------|---------------------|---------|---|--|--|---|--|
|                                 | maintenance [1.2.6]<br>j. Information security incident management [1.2.7]<br>k. Business continuity management [section 8.2]<br>l. Compliance [sections 1 and 10]  |                |                     |         |   |  |  |   |  |
| Logical Access Controls (8.2.2) | Logical access to personal information is restricted by procedures that address the following matters:<br>a. Authorizing and registering internal personnel and individuals<br>b. Identifying and authenticating internal personnel and individuals<br>c. Making changes and updating access profiles<br>d. Granting privileges and permissions for access to IT infrastructure components and personal information<br>e. Preventing individuals from accessing anything other than their own personal or sensitive information<br>f. Limiting access to personal information only to authorized internal personnel based upon their assigned roles and responsibilities<br>g. Distributing output only to authorized internal personnel<br>h. Restricting logical access to offline storage, backup data, systems and media<br>i. Restricting access to system configurations, superuser functionality, master passwords, powerful utilities, and security devices (for example, firewalls)<br>j. Preventing the | Security       | 3                   | Defined | Controls over access and privileges to files and databases containing personal information are informal, inconsistent and incomplete. | The entity has basic security procedures; however, they do not include specific requirements governing logical access to personal information and may not provide an appropriate level of access or control over personal information. | <b>The entity has documented and implemented security policies and procedures that sufficiently control access to personal information.</b><br><br><b>Access to personal information is restricted to employees with a need for such access.</b> | Management monitors logical access controls, including access attempts and violation reports for files, databases and resources containing personal information to identify areas where additional security needs improvement.<br><br>Irregular access of authorized personnel is also monitored. | Access and violation attempts are assessed to determine root causes and potential exposures and remedial action plans are developed and implemented to increase the level of protection of personal information. Logical access controls are continually assessed and improved.<br><br>Irregular access of authorized personnel is monitored, assessed and investigated where necessary. |

| GAPP Criteria                    | Criteria Description   | CFPB Principle | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined   | Managed  | Optimized  |  |
|----------------------------------|--|----------------|---------------------|------------|--|---|--|--|--|
|                                  | introduction of viruses, malicious code, and unauthorized software   |                |                     |            |  |   |  |  |  |
| Physical Access Controls (8.2.3) | Physical access is restricted to personal information in any form (including the components of the entity's system(s) that contain or protect personal information). | Security       | 3                   | Defined    | Controls over physical access to personal information are informal, incomplete and inconsistent.   | The entity has basic physical security procedures; however, they do not include specific requirements governing physical access to personal information maintained or stored in various media. Accordingly, inconsistent approaches are taken throughout the entity with respect to physically securing personal information. | <b>The entity has implemented formal physical security policies and procedures that form the basis of specific privacy-related security procedures for physical access to personal information.</b><br><br><b>Physical access to personal information is restricted to employees with a need for such access.</b>  | Management monitors physical access controls. Personal information is physically stored in secure locations. Access to such locations is restricted and monitored. Unauthorized access is investigated and appropriate action taken. | Where physical access or attempted violation of personal information has occurred, the events are analyzed and remedial action including changes to policies and procedures is adopted. This may include implementing increased use of technology, as necessary. Physical access controls are continually assessed and improved. |
| Environmental Safeguards (8.2.4) | Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.                                   | Security       | 2                   | Repeatable | Some policies and procedures exist to ensure adequate safeguards over personal information in the event of disasters or other environmental hazards; however, they are incomplete and inconsistently applied. The entity may lack a business continuity plan that would require an assessment of threats and vulnerabilities and appropriate protection of personal information. | <b>The entity has a business continuity plan addressing certain aspects of the business. Such a plan may not specifically address personal information. Accordingly, personal information may not be appropriately protected. Business continuity plans are not well documented and have not been tested.</b>                 | The entity has implemented a formal business-continuity and disaster-recovery plan that address all aspects of the business and identified critical and essential resources, including personal information in all forms and media, and provides for specifics thereof. Protection includes protection against accidental, unauthorized or inappropriate access or disclosure of personal information. The plan has been tested. | Management monitors threats and vulnerabilities as part of a business risk management program and, where appropriate, includes personal information as a specific category.  | Management risk and vulnerability assessments with respect to personal information result in improvements to the protection of such information.   |

| GAPP Criteria                                  | Criteria Description  | CFPB Principle | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined  | Managed   | Optimized   |   |
|--|---|----------------|---------------------|------------|---|--|---|---|---|
| Transmitted Personal Information (8.2.5)       | Personal information is protected when transmitted by mail or other physical means. Personal information collected and transmitted over the Internet, over public and other non-secure networks, and wireless networks is protected by deploying industry-standard encryption technology for transferring and receiving personal information. | Security       | 2                   | Repeatable | The protection of personal information when being transmitted or sent to another party is informal, incomplete and inconsistently applied. Security restrictions may not be applied when using different types of media to transmit personal information. | Policies and procedures exist for the protection of information during transmittal but are not fully documented; however, they may not specifically address personal information or types of media.  | Documented procedures that cover all relevant aspects have been implemented and are working effectively to protect personal information when transmitted.   | The entity's policies and procedures for the transmission of personal information are monitored to ensure that they meet minimum industry security standards and the entity is in compliance with such standards and their own policies and procedures. Issues of non-compliance are dealt with.  | Management reviews advances in security technology and techniques and updates their security policies and procedures and supporting technologies to afford the entity the most effective protection of personal information while it is being transmitted, regardless of the media used.  |
| Personal Information on Portable Media (8.2.6) | Personal information stored on portable media or devices is protected from unauthorized access.   | Security       | 4                   | Managed    | Controls over portable devices that contain personal information are informal, incomplete and inconsistent.   | Procedures are in place to protect personal information on portable devices; however, they are not fully documented. Employees are aware of the additional risks and vulnerabilities associated with the use of portable and removable devices. Awareness of requirements to protect personal information are known and certain procedures exist to preclude or restrict the use of portable and removal devices to record, transfer and archive personal information. | The entity has implemented documented policies and procedures, supported by technology, that cover all relevant aspects and restrict the use of portable or removable devices to store personal information. The entity authorizes the devices and requires mandatory encryption. | <b>Prior to issuance of portable or removable devices, employees are required to read and acknowledge their responsibilities for such devices and recognize the consequences of violations of security policies and procedures. Where portable devices are used, only authorized and registered devices such as portable flash drives that require encryption are permitted. Use of unregistered and unencrypted portable devices is not allowed in the entity's computing environment.</b> | Management monitors new technologies to enhance the security of personal information stored on portable devices. They ensure the use of new technologies meets security requirements for the protection of personal information, monitor adoption and implementation of such technologies and, where such monitoring identifies deficiencies or exposures, implement remedial action. |

| GAPP Criteria                        | Criteria Description   | CFPB Principle             | CFPB Maturity Level | Ad Hoc   | Repeatable   | Defined   | Managed  | Optimized  |
|--------------------------------------|--|----------------------------|---------------------|--|--|---|--|--|
| Testing Security Safeguards (8.2.7)  | Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted at least annually.  | Accountability & Auditing  | 3 Defined           | Tests of security safeguards for personal information are undocumented, incomplete and inconsistent.   | Periodic tests of security safeguards are performed by the IT function; however, their scope varies.   | Periodic and appropriate tests of security safeguards for personal information are performed in all significant areas of the business. Test work is completed by qualified personnel such as Certified Public Accountants, Chartered Accountants, Certified Information System Auditors, or internal auditors. Test results are documented and shared with appropriate stakeholders. Tests are performed at least annually. | Management monitors the testing process, ensures tests are conducted as required by policy, and takes remedial action for deficiencies identified.                             | Test results are analyzed, through a defined root-cause analysis, and remedial measures documented and implemented to improve the entity's security program.                     |
| QUALITY (4 criteria)                 | The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.   |                            |                     |  |  |   |  |  |
| Privacy Policies (9.1.0)             | The entity's privacy policies address the quality of personal information.   | Data quality and integrity | 2 Repeatable        | Quality control policies and procedures exist informally.  | Quality provisions in privacy policies exist, but may not cover all aspects and are not fully documented.  | Quality provisions in privacy policies cover all relevant aspects and are fully documented.   | Compliance with quality provisions in privacy policies and procedures is monitored and the results are used to reinforce key privacy messages.                                 | Management monitors compliance with privacy policies and procedures relating to quality. Issues of non-compliance are identified and remedial action taken to ensure compliance. |
| Communication to Individuals (9.1.1) | Individuals are informed that they are responsible for providing the entity with accurate and complete personal information and for contacting the entity if correction of such information is required. | Openness & Transparency    | 3 Defined           | Individuals may be informed about their responsibility to provide accurate and complete personal information; however, communications are inconsistent, sporadic and undocumented. | Individuals are informed of their responsibility to provide accurate information; however, communications may not cover all aspects and may not be fully documented. | Individuals are informed of their responsibility for providing accurate and complete personal information and for contacting the entity if corrections are necessary. Such communications cover all relevant aspects and are documented.  | Communications are monitored to ensure individuals are adequately informed of their responsibilities and the remedies available to them should they have complaints or issues. | Communications are monitored and analyzed to ensure the messaging is appropriate and meeting the needs of individuals and changes are being made where required.                 |

| GAPP Criteria   | Criteria Description  | CFPB Principle             | CFPB Maturity Level | Ad Hoc     | Repeatable  | Defined  | Managed  | Optimized   |   |
|---|---|----------------------------|---------------------|------------|---|--|--|---|---|
| Accuracy and Completeness of Personal Information (9.2.1) | Personal information is accurate and complete for the purposes for which it is to be used.  | Data quality and integrity | 2                   | Repeatable | Procedures exist to ensure the completeness and accuracy of information provided to the entity; however, they are informal, incomplete and inconsistently applied.                | Procedures are in place to ensure the accuracy and completeness of personal information; however, they are not fully documented and may not cover all aspects.                           | Documented policies, procedures and processes that cover all relevant aspects have been implemented to ensure the accuracy of personal information. Individuals are provided with information on how to correct data the entity maintains about them.  | Processes are designed and managed to ensure the integrity of personal information is maintained. Benchmarks have been established and compliance measured. Methods are used to verify the accuracy and completeness of personal information obtained, whether from individuals directly or from third parties. | Processes are in place to monitor and measure the accuracy of personal information. Results are analyzed and modifications and improvements made.   |
| Relevance of Personal Information (9.2.2)                 | Personal information is relevant to the purposes for which it is to be used.  | Data quality and integrity | 3                   | Defined    | Some procedures are in place to ensure the personal information being collected is relevant to the defined purpose, but they are incomplete, informal and inconsistently applied. | Procedures are in place to ensure that personal information is relevant to the purposes for which it is to be used, but these procedures are not fully documented nor cover all aspects. | Documented policies and procedures that cover all relevant aspects, supported by effective processes, have been implemented to ensure that only personal information relevant to the stated purposes is used and to minimize the possibility that inappropriate information is used to make business decisions about the individual. | Processes are designed and reviewed to ensure the relevance of the personal information collected, used and disclosed.  | Processes are in place to monitor the relevance of personal information collected, used and disclosed. Results are analyzed and modifications and improvements made as necessary.                   |
| MONITORING and ENFORCEMENT (7 criteria)                   | The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related inquiries, complaints and disputes. |                            |                     |            |   |  |  |   |   |
| Privacy Policies (10.1.0)                                 | The entity's privacy policies address the monitoring and enforcement of privacy policies and procedures.  | Accountability & Auditing  | 2                   | Repeatable | Monitoring and enforcement of privacy policies and procedures are informal and ad hoc. Guidance on conducting such reviews is not documented.                                     | Monitoring and enforcement provisions in privacy policies and procedures exist but may not cover all aspects, and are not fully documented.  | Monitoring and enforcement provisions in privacy policies cover all relevant aspects and are fully documented.   | Compliance with monitoring and enforcement provisions in privacy policies is monitored and results are used to reinforce key privacy messages.  | Management monitors compliance with privacy policies and procedures relating to monitoring and enforcement. Issues of non-compliance are identified and remedial action taken to ensure compliance. |

| GAPP Criteria                                   | Criteria Description  | CFPB Principle            | CFPB Maturity Level | Ad Hoc  | Repeatable  | Defined  | Managed  | Optimized   |  |
|---|---|---------------------------|---------------------|---------|---|--|--|---|--|
| Communication to Individuals (10.1.1)           | Individuals are informed about how to contact the entity with inquiries, complaints and disputes. | Accountability & Auditing | 3                   | Defined | Individuals may be informed about how to contact the entity with inquiries, complaints and disputes; however, communications are inconsistent, sporadic and undocumented. | Procedures are in place to inform individuals about how to contact the entity with inquiries, complaints, and disputes but may not cover all aspects and are not fully documented. | Individuals are informed about how to contact the entity with inquiries, complaints and disputes and to whom the individual can direct complaints. Policies and procedures are documented and implemented.   | Communications are monitored to ensure that individuals are adequately informed about how to contact the entity with inquiries, complaints and disputes.  | Communications are monitored and analyzed to ensure the messaging is appropriate and meeting the needs of individuals and changes are being made where required. Remedial action is taken when required. |
| Inquiry, Complaint and Dispute Process (10.2.1) | A process is in place to address inquiries, complaints and disputes.                              | Individual participation  | 4                   | Managed | An informal process exists to address inquiries, complaints and disputes; however, it is incomplete and inconsistently applied.   | Processes to address inquiries, complaints and disputes exist, but are not fully documented and do not cover all aspects.  | Documented policies and procedures covering all relevant aspects have been implemented to deal with inquiries, complaints and disputes. Inquiries, complaints and disputes are recorded, responsibilities assigned and addressed through a managed process. Recourse and a formal escalation process are in place to review and approve any recourse offered to individuals. | Management monitors and analyzes the process to address inquiries, complaints and disputes and makes changes to the process, where appropriate.   |  |
| Dispute Resolution and Recourse (10.2.2)        | Each complaint is addressed, and the resolution is documented and communicated to the individual. | Individual participation  | 3                   | Defined | Complaints are handled informally and inconsistently. Adequate documentation is not available.  | Processes are in place to address complaints, but they are not fully documented and may not cover all aspects.   | Documented policies and procedures covering all relevant aspects have been implemented to handle privacy complaints. Resolution of the complaints is documented.   | Privacy complaints are reviewed to ensure they are addressed within a specific timeframe in a satisfactory manner; satisfaction is monitored and managed. Unresolved complaints are escalated for review by management. | Privacy complaints are monitored and analyzed and the results used to redesign and improve the privacy complaint process.  |

| GAPP Criteria                       | Criteria Description  | CFPB Principle            | CFPB Maturity Level | Ad Hoc     | Repeatable   | Defined   | Managed   | Optimized  |  |
|-------------------------------------|---|---------------------------|---------------------|------------|--|---|---|--|--|
| Compliance Review (10.2.3)          | Compliance with privacy policies and procedures, commitments and applicable laws, regulations, service level agreements and other contracts is reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented. | Accountability & Auditing | 2                   | Repeatable | Review of compliance with privacy policies and procedures, laws, regulations and contracts is informal, inconsistently and incomplete. | Policies and procedures to monitor compliance with privacy policies and procedures, legislative and regulatory requirements and contracts are in place, but are not fully documented and may not cover all aspects.                         | Documented policies and procedures that cover all relevant aspects have been implemented that require management to review compliance with the entity's privacy policies and procedures, laws, regulations, and other requirements.             | Management monitors activities to ensure the entity's privacy program remains in compliance with laws, regulations and other requirements.                           | Management analyzes and monitors results of compliance reviews of the entity's privacy program and proactively initiates remediation efforts to ensure ongoing and sustainable compliance.   |
| Instances of Noncompliance (10.2.4) | Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.   | Accountability & Auditing | 2                   | Repeatable | Processes to handle instances of noncompliance exist, but are incomplete, informal and inconsistently applied.                         | Policies and procedures are in place to document non-compliance with privacy policies and procedures, but are not fully documented or do not cover all relevant aspects. Corrective and disciplinary measures may not always be documented. | Documented policies and procedures covering all relevant aspects have been implemented to handle instances of non-compliance with privacy policies and procedures. Corrective and disciplinary measures of non-compliance are fully documented. | Management monitors noncompliance with privacy policies and procedures and takes appropriate corrective and disciplinary action in a timely fashion.                 | Non-compliance results in disciplinary action and remedial training to correct individual behavior. In addition policies and procedures are improved to assist in full understanding and compliance.                               |
| Ongoing Monitoring (10.2.5)         | Ongoing procedures are performed for monitoring the effectiveness of controls over personal information based on a risk assessment and for taking timely corrective actions where necessary.  | Accountability & Auditing | 2                   | Repeatable | Ongoing monitoring of privacy controls over personal information is informal, incomplete and inconsistently applied.                   | Monitoring of privacy controls is not fully documented and does not cover all aspects   | The entity has implemented documented policies and procedures covering all relevant aspects to monitor its privacy controls. Selection of controls to be monitored and frequency with which they are monitored are based on a risk assessment.  | Monitoring of controls over personal information is performed in accordance with the entity's monitoring guidelines and results analyzed and provided to management. | Monitoring is performed and the analyzed results are used to improve the entity's privacy program. The entity monitors external sources to obtain information about their privacy "performance" and initiates changes as required. |

## Section 3: Travel Policy

---

### 3.1 Scope of Audit

As an independent executive agency, CFPB has in principle chosen to follow the Federal Travel Regulation (FTR) and most aspects of the FTR were implemented for FY12. Further, CFPB has developed its own travel policy—incorporating regulatory requirements—and has established a designated office for processing travel vouchers and travel card requests. The Bureau currently uses GovTrip to process travel claims and also relies on the Bureau of Public Debt (BPD) systems to record and pay travel claims timely. CFPB has determined that it is not limited solely to follow Parts 302 and 303 of the FTR if this results in a conflict with its statutory obligation under Section 1013(a)(2) of the Consumer Financial Protection Act (CFPA) to provide compensation and benefits comparable to the compensation and benefits being provided by the Board of Governors for the corresponding class of employees. We have been informed that until a new travel policy is developed, the Bureau will continue to implement the FTR.

The scope of this audit is defined by three key factors: (1) the set of Federal requirements and regulations governing travel policy, (2) policies and procedures that CFPB has established to date, with respect to travel policies and processes; and (3) the future-state that CFPB has planned in this area, taking into account Federal standards and best practices. The goal of this assessment is to evaluate CFPB’s travel policy, systems and processes and make recommendations for improving their effectiveness and efficiency for the organization, where applicable.

With this in mind, we reviewed the organizational structures, business processes, policy communications, and technology systems that have been established to support travel policy operations and administration within the CFPB. We also reviewed draft policies and procedures that have been formulated to further define rules around travel and travel card use. Specifically, the scope of our work included the following:

- Review of CFPB travel policy and procedures documentation;
- Understanding of the operational systems (both CFPB specific and government-wide) that are being used;
- Evaluation of the process for authorizing travel plans; preparing and reporting travel claims; processing and paying travel advances and expenses; and conducting post-payment audits;
- Assessment of CFPB travel operations relative to Federal standards and guidelines;
- Assessment of the risk of incurring inappropriate expenses as travel claims; and
- Status of corrective action plans for addressing GAO’s findings and recommendations from the audit of fiscal year 2011 financial statements

### 3.2 Evaluation Criteria

The purpose of the section is to describe the evaluation criteria for this review area. As with other areas of performance, our audit focuses on three sets of criteria: (1) compliance with legal requirements; (2) achievement of organizational goals; and (3) alignment with performance standards, best practices, and/or benchmarks.

### **3.2.1 Compliance with the Law**

The ASR Team evaluated CFPB's performance against applicable sections of the law and related regulations, including the Travel and Transportation Reform Act (TTRA) of 1998 (Public Law 105-264), and the Federal Travel Regulation (FTR) contained in Chapters 300 through 304 of Code of Federal Regulations (CFR). Specifically, we examined the CFPB's performance against the following FTR provisions:

- Federal employees must use the government travel charge card for payment of expenses related to official government travel.
- The agency should reimburse employees who submit a proper travel voucher for allowable travel expenses in accordance with applicable travel regulations within 30 days after submission of a proper voucher.
- Agencies (as defined in §301-1.1 of the CFR) that spend more than \$5 million on travel and transportation payments during a fiscal year may also need to comply with certain reporting requirements—for example, an agency must report the total amount of such payments in a given year, if included in a GSA survey sample.

### **3.2.2 Achievement of Organizational Goals**

CFPB performance standards for travel require that official travel is conducted in a responsible manner with minimum costs, and that travel related policies are clearly communicated within the agency and to its employees. Guidance must be provided in the following areas:

- Issuance and control of travel cards
- Travel authorization
- Request and approval of travel advances and documentation
- Preparation of travel vouchers
- Approval of allowable travel expenses
- Audit of travel expenses before payment
- Post payment audit

Comprehensive guidance must include local travel, temporary change of station, permanent change of station and Non-Federal sponsored travel.

CFPB must also minimize the reputational risk of incurring inappropriate expenses by instituting proper compliance and monitoring controls, yet it must aim to facilitate and improve the travel process and improve employee satisfaction.

Under Section 1017(a)(4)(E) of the CFPA, the CFPB is generally not required to follow OMB guidance or consult with or obtain the approval of OMB with respect to Bureau affairs or operations. Nevertheless, CFPB has chosen as a matter of policy to follow particular OMB guidance as a matter of best practice, such as OMB Circular A-123 Appendix B. In such instances, adherence to the guidelines is considered to be an organization goal for the purposes of this audit.

For example, OMB Circular A-123 Appendix B advises agencies to develop and maintain written policies and procedures for the appropriate use of charge cards, consistent with the requirements of the Circular. It also requires implementation of risk management controls, policies and practices consistent with the requirements—to ensure the efficiency and integrity of charge card programs by eliminating payment delinquencies, charge card misuse, fraud, and other forms of waste and abuse.

The GSA SmartPay Program manages a set of master contracts through which agencies and organizations, including CFPB, obtain charge cards for employees to accomplish the agency or organization's mission. CFPB Travel strategy and organization reflect the GSA SmartPay regulations, and travel cards are used specifically to pay for travel related expenses for government employees on official government travel. Travel cards come in two types, centrally billed account (CBA) and individually billed accounts (IBA).

In addition to the goals outlined above, GAO identified certain opportunities for improvement that could adversely affect CFPB's ability to meet the performance objectives and standards in this area. Based on its findings during the audit of fiscal year 2011 financial statements, GAO recommended the following:

- CFPB must implement procedures to ensure that amendments to travel relocation obligations are recorded in the proper period as part of ensuring the accuracy of obligation balances,
- CFPB must enhance its travel policies and procedures to expressly state that prior written approval be obtained for all reimbursed travel expenses, and
- CFPB must issue a memorandum to all CFPB staff for obtaining prior written approval for all travel expenses that are reimbursed.

CFPB currently uses GovTrip to process travel claims, and is considering migration to a new GSA e-travel system. Once these plans and requirements are clearly established, a key goal for the travel organization will be to implement the new system and train all travelers in using this system.

### **3.2.3 Alignment with Performance Standards and Best Practices**

As stated earlier, under Section 1017(a)(4)(E) of the CFPA, the CFPB is not required to follow OMB guidance or consult with or obtain the approval of OMB with respect to Bureau affairs or operations. Nevertheless, the underlying practices in certain OMB circulars pertaining to travel can be viewed as leading practices. Where appropriate, other relevant benchmarks, including those for assessing and improving traveler satisfaction, have been cited to guide future performance of the agency's travel operations. While CFPB is not required by statute to comply with these regulations, it may choose to do so as a matter of policy. For instance, Treasury Financial Manual, Part 4, Chapter 4500 provides guidelines that each agency must develop its own internal procedures for using purchase cards for small purchases, and put in place processing and internal controls prior to using government cards. In addition to compliance with standards that will assist in the improvement of travel related areas, management systems and risk management practices that are in place were also evaluated during the course of our work.

### 3.3 Findings and Recommendations

In this section, we present findings and recommendations related to CFPB’s travel policy. In general, we found that CFPB is compliant with the legal requirements of the TTRA, documented policy guidance is in place, and internal controls are operational and consistent with the requirements of the GSA SmartPay and FTR.

Within this review area, we examined the Bureau’s performance with respect to 12 total performance elements. The audit team provided no recommendations or suggestions for 9 of the 12 performance elements (75%), indicating that there were no significant performance issues in these areas and no identified opportunities for improvement. The remaining performance elements are addressed through 3 performance improvement opportunities. We identified no significant performance issues.

#### 3.3.1 Performance Improvement Opportunities

Below, we present information on aspects of performance related to performance issues that we believe could be improved, but do not require corrective action. For each of these performance improvement opportunities, we offer suggestions for future action, and we summarize the criteria on which these suggestions are based.

**2012.TR.1 State Estimated Expenditure on Travel Requests and Required Approval of Travel Vouchers by the Supervisor.** OMB Circular A-123, Appendix B “Improving the Management of Government Charge Card Programs” defines the role of the Approving Official (AO), stating that the AO “(typically a supervisor) ensures that the purchase card is used properly” and “authorizes cardholder purchases (for official use only)...” The OMB guidance goes on to state that the AO “signs the travel voucher, indicating approval for payment and for its content.”<sup>8</sup>

While the travel authorization currently used by the Bureau captures the most significant travel costs (i.e., estimated costs of ticketed travel, lodging, and rental vehicles), the authorization does not provide a comprehensive estimated dollar amount to be expended on the trip. Thus, travel requests are approved by the Supervisor without requiring all pertinent information. CFPB has deliberately centralized in the Travel Office the process of approving travel authorizations and reimbursement vouchers—applying a series of standard checks throughout the process, which apply in a uniform fashion across the Bureau, to ensure accountability at every stage of the travel expense approval process.

To enhance oversight and control of Bureau staff travel, we recommend that a comprehensive estimated dollar amount be stated in the initial authorization and approved by the Supervisor of the traveler. CFPB should further strengthen accountability and timing of internal control oversight by instituting Supervisor approval of the Travel Voucher before the voucher is routed to the Travel Office for review and payment.

**2012.TR.2 Completion and Approval of Relocation Expenses Policy.** While the CFPB Policy for Travel Cards and Temporary Travel Duty is finalized and approved, the Relocation Expenses Policy document is in an interim draft stage. We recommend that the interim Relocation Expenses Policy and the rules governing such expenditure be finalized and approved to provide final authoritative sources for both travel related matters.

---

<sup>8</sup> OMB Circular A-123, Appendix B (Revised, January 15, 2009), Attachment 1 – Glossary.

**2012.TR.3 Enhancement of Travel Cards and Temporary Travel Duty Policy.** The Policy for Travel Cards and Temporary Travel Duty does not provide clear guidance on matters such as: (1) expense documentation and record retention requirements; and (2) recovery of travel cards upon termination. We recommend that CFPB enhance its current travel policy to incorporate these elements, in accordance with OMB Circular A-123, Appendix B, “Improving the Management of Government Charge Card Programs” to provide comprehensive authoritative guidance to agency staff.

### **3.3.2 Summary of Demonstrated Performance**

Table 3 presents information on the Bureau’s demonstrated performance and achievements across all 13 performance elements that were audited in this review area.

**Table 3: Summary of Demonstrated Performance**

| Performance Requirement or Standard  | Demonstrated Performance  | Recommendation or Performance Improvement Opportunity                  |
|--|---|--|
| <b>Compliance with the Law</b>   |   |  |
| <p>TRAVEL AND TRANSPORTATION REFORM ACT OF 1998<br/>SEC. 2. REQUIRING USE OF THE TRAVEL CHARGE CARD.</p> <p>(a) IN GENERAL.— Under regulations issued by the Administrator of General Services after consultation with the Secretary of the Treasury, the Administrator shall require that Federal employees use the travel charge card established pursuant to the United States Travel and Transportation Payment and Expense Control System, or any Federal contractor-issued travel charge card, for all payments of expenses of official Government travel.</p>   | <ul style="list-style-type: none"> <li>• CFPB has implemented the General Services Administration (GSA) SmartPay Travel Card program with Citibank.</li> <li>• Approximately 570 travel cards are currently in use.</li> <li>• CFPB has a Policy on Travel Cards and Temporary Travel Duty.</li> <li>• Travel cards are used only to pay for travel related expenses for government employees on official government travel.</li> <li>• Travel cards come in two types, centrally billed account (CBA) and individually billed accounts (IBA).</li> </ul>                                 | <p>No recommendations provided for this performance audit element.</p> |
| <p>(f) REPORTS.—</p> <p>(1) IN GENERAL.—The Administrator of General Services shall submit 2 reports to the Congress on agency compliance with this section and regulations that have been issued under this section.</p> <p>(2) TIMING.—The first report under this subsection shall be submitted before the end of the 180-day period beginning on the date of the enactment of this Act, and the second report shall be submitted after that period and before the end of the 540-day period beginning on that date of enactment.</p> <p>(3) PREPARATION.—Each report shall be based on a sampling survey of agencies that expended more than \$5,000,000 during the previous fiscal year on travel and transportation payments, including payments for employee relocation. The head of an agency shall provide to the Administrator the necessary information in a format prescribed by the Administrator and</p> | <ul style="list-style-type: none"> <li>• For FY11, CFPB was not required to report survey data to GSA, as the amount of travel expenditure for the fiscal year was below the threshold of \$5 million.</li> <li>• The extent of travel has increased significantly in the current year as CFPB has ramped up its staffing and number of examinations.</li> <li>• For FY12, travel expenditures are expected to exceed the \$5M threshold, based on expenditure during the first nine months of the year. CFPB is taking steps to provide the survey data, if requested by GSA.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard  | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity                  |
|--|--|--|
| <p>approved by the Director of the Office of Management and Budget.</p>  |  |  |
| <p>(g) REIMBURSEMENT OF TRAVEL EXPENSES.— In accordance with regulations prescribed by the Administrator of General Services, the head of an agency shall ensure that the agency reimburses an employee who submits a proper voucher for allowable travel expenses in accordance with applicable travel regulations within 30 days after submission of the voucher. If an agency fails to reimburse an employee who has submitted a proper voucher within 30 days after submission of the voucher, the agency shall pay the employee a late payment fee as prescribed by the Administrator.</p>  | <ul style="list-style-type: none"> <li>• Travel Vouchers deemed "proper" are reimbursed to employees within 30 days to meet this requirement and also the requirement of the Prompt Payment Act.</li> </ul>  | <p>No recommendations provided for this performance audit element.</p> |
| <p>SEC. 3. PREPAYMENT AUDITS OF TRANSPORTATION EXPENSES.</p> <p>(3) Section 3726 of title 31, United States Code, is amended —</p> <p>(A) by amending subsection (a) to read as follows:</p> <p>“(a)(1) Each agency that receives a bill from a carrier or freight forwarder for transporting an individual or property for the United States Government shall verify its correctness (to include transportation rates, freight classifications, or proper combinations thereof ), using prepayment audit, prior to payment in accordance with the requirements of this section and regulations prescribed by the Administrator of General Services.</p> | <ul style="list-style-type: none"> <li>• Current CFPB Policy COO-038 – Policy on Travel Cards and Temporary Travel Duty requires travelers to adhere to the GSA SmartPay program and the Federal Travel Regulation (FTR).</li> <li>• An Interim Relocation Expenses Policy has been documented.</li> <li>• Travel Vouchers and expenditures are checked by the Approving Officials in the Office of Travel prior to payment.</li> <li>• CFPB has determined that it is not required to follow Parts 302 and 303 of the FTR, in cases where it results in a conflict with its statutory obligation under Section 1013(a)(2) of Dodd-Frank to provide compensation and benefits comparable to the compensation and benefits being provided by the Board of Governors of the Federal Reserve for the corresponding class of employees.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |
| <p><b>Achievement of Organizational Goals</b></p>  |  |  |
| <p>Travel strategy and organization reflect the GSA SmartPay regulations and the Federal Travel Regulations (particularly Chapter 301), and also other benefits in accordance with Dodd-Frank.</p>   | <ul style="list-style-type: none"> <li>• Policy on Travel Cards and Temporary Travel Duty requires compliance with GSA SmartPay program and FTR.</li> <li>• The CFPB employee is responsible to pay for any charges</li> </ul>   | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity                  |
|---|--|--|
|   | <p>or expenses not associated with FTR or business purposes.</p> <ul style="list-style-type: none"> <li>• CFPB employees undergo training to familiarize themselves with GSA SmartPay requirements.</li> <li>• GSA SmartPay travel charge card may be used for authorized official travel and authorized travel related expenses only. Official travel expenses are transportation, lodging, meals, and incidentals.</li> <li>• An Agency/Organization Program Coordinator (A/OPC) has been appointed and undergone training for the Travel Card Program.</li> <li>• GSA approved GovTrip, which is hosted by Treasury BPD, is currently the system of choice for processing all travel actions.</li> <li>• Approving Official in the Office of Travel validates Travel Vouchers for adherence to FTR/GSA per diem rates for temporary duty travel.</li> </ul>               |  |
| <p>CFPB aims to facilitate and improve the travel process, and improve employee satisfaction with this process.</p> | <ul style="list-style-type: none"> <li>• CFPB conducted an employee survey in September 2011 to obtain feedback on its processes.</li> <li>• In this survey, the travel process was voted as the number 2 pain point within the organization. The major problems identified were cumbersome approval process, lack of blanket approval for frequent travelers, complicated process, and problems with GovTrip.</li> <li>• Office of Strategy captured the raw data and performed analysis on this data. An initial update based on this analysis was provided in September 2011 by the Office of Strategy</li> <li>• Remediation action commenced with the introduction of Limited Open Travel Authorization (LOTA) forms in June 2012 and these changes were incorporated in the travel policy.</li> <li>• GSA is working to replace the currently used e-travel</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Performance Improvement Opportunity  |
|---|---|--|
| <p>CFPB takes appropriate steps to mitigate reputational risk due to misuse and improper use of travel funds, especially misuse of travel cards, which have automated teller machine (ATM) access.</p>  | <p>systems including GovTrip with another e-travel system.</p> <ul style="list-style-type: none"> <li>• Travel Policy for local travel has been documented and implemented.</li> <li>• Travel information is available on the CFPB website and includes Frequently Asked Questions (FAQs).</li> <li>• LOTA forms were introduced by the COO in the CFPB Weekly Operations Division Digest, together with a number of other items.</li> <li>• Travel Card holders complete online GSA SmartPay training.</li> <li>• Travelers' supervisor approves travel requests.</li> <li>• An Approving Official in the Office of Travel verifies and validates expenses prior to payment.</li> <li>• Treasury BPD performs post payment audit on a random sample of vouchers and provides quarterly reports on the results of these audits.</li> <li>• The post payment audit process reported a number of findings for the first quarter of FY12, which has been reduced to no finding for the 2nd Quarter and one finding for the 3rd Quarter.</li> <li>• The Director of Travel performs corrective action on any post payment audit findings and recovers amounts claimed improperly, if required.</li> </ul> | <p>Additional Action Suggested</p> <p>2012.TR.1 (Performance Improvement Opportunity): The travel request is approved by the Supervisor without any knowledge of the estimated dollar amount to be expended on the trip. Further, Travel Vouchers are not routed for approval by the traveler's Supervisor. We recommend that the dollar amount be stated in the initial travel request and approved by the Supervisor. Additionally, CFPB should strengthen internal control by instituting approval of the Travel Voucher by the Supervisor before it is routed to the Approving Official in the Office of Travel for payment.</p> |
| <p>CFPB currently uses GovTrip to process travel claims, and is considering migration to a new GSA e-travel system. Once these plans and requirements are clearly established, a key goal for the travel organization will be to implement the new system and train all travelers in using this system.</p> | <ul style="list-style-type: none"> <li>• CFPB is currently using the system adopted by Treasury BPD.</li> <li>• CFPB is reviewing whether it is obligated to use GovTrip or any other GSA e-travel system, which may impact future travel operations.</li> <li>• GSA has completed its assessment and is looking forward to contracting for a new e-travel system for use by federal agencies.</li> </ul>   | <p>No recommendations provided for this performance audit element.</p>   |
| <p>GAO identified certain internal control issues that adversely affect</p>   | <ul style="list-style-type: none"> <li>• A communication, dated July 6, 2012, from the CFPB CFO</li> </ul>  | <p>No recommendations provided for this performance</p>  |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Performance Improvement Opportunity  |
|---|--|--|
| <p>CFPB's ability to meet the performance objectives and standards in this area. Based on its findings during the audit of fiscal year 2011 financial statements, corrective action is required for the following recommendations:</p> <ul style="list-style-type: none"> <li>• CFPB must implement procedures to ensure that amendments to travel relocation obligations are recorded in the proper period as part of ensuring the accuracy of obligation balances,</li> <li>• CFPB must enhance its travel policies and procedures to expressly state that prior written approval be obtained for all reimbursed travel expenses, and</li> <li>• CFPB must issue a memorandum to all CFPB staff for obtaining prior written approval for all travel expenses that are reimbursed, and implement documentation to support the approval of these expenses.</li> </ul> | <p>to Congress outlined planned implementation of the GAO recommendations.</p> <ul style="list-style-type: none"> <li>• The Travel Policy was enhanced to include a Travel Approval Form. This form replaced the Supervisor's approval in GovTrip. This form is signed by the approver and attached (in PDF format) to the travel authorization in GovTrip.</li> <li>• Agency-wide communication for the change in approval documentation was made by the Director of Travel on May 4, 2012.</li> <li>• A Recording Commitments and Obligations Policy has been documented.</li> <li>• The Office of Travel follows up outstanding obligations towards the year end to ensure that outstanding travel vouchers are submitted.</li> <li>• According to CFPB officials, BPD/ARC has instructed Contracting Officers to ensure the prompt entry of obligation documents into PRISM to ensure recording of obligations in the correct period.</li> </ul> | <p>audit element.</p>  |
| <p>Implement OMB Circular A-123 Appendix B guidance and improve internal control on travel cards including guidance on the following:</p> <ul style="list-style-type: none"> <li>• Description of Agency training requirements,</li> <li>• Monitoring misuse and delinquencies,</li> <li>• Performance metrics, spend analysis, delinquency rates and other relevant transactions and program management issues,</li> <li>• Recovery of travel cards upon termination of employees, and</li> <li>• CFPB policy with respect to administrative and/or disciplinary actions, including when referral to an agency Office of Inspector General is appropriate or required.</li> </ul>  | <ul style="list-style-type: none"> <li>• GSA SmartPay and GovTrip training is provided.</li> <li>• The Employee Out-processing Checklist for terminations includes a request to contact A/OPC for CFPB travel card and outstanding Travel Vouchers.</li> <li>• CBA statements are reconciled to Oracle Financials data and GovTrip before payment.</li> <li>• Monthly reports of delinquent payments are received from Citibank and reported to the traveler for settlement.</li> <li>• Travel card responsibility lies with the cardholder, including settlement of delinquent payments.</li> <li>• CFPB reports that there have been no instances of</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.TR.2 (Performance Improvement Opportunity: The Policy On Travel Cards and Temporary Travel Duty does not provide clear guidance on matters such as travel card training requirements, expense documentation and record retention requirements, recovery of travel cards upon termination, and administrative and disciplinary actions for misuse. We recommend that CFPB enhance its current travel policy to incorporate these elements.</p> |

| Performance Requirement or Standard                            | Demonstrated Performance  | Recommendation or Performance Improvement Opportunity   |
|--|---|---|
|  | fraudulent use of travel card reported to the OIG. There has been one termination.  |   |
| <b>Alignment with Performance Standards and Best Practices</b> |   |   |
| Compliance with standards and guidelines                       | <ul style="list-style-type: none"> <li>• CFPB has developed its own internal policy and procedures for using purchase cards.</li> <li>• CFPB Travel Card policy and procedures closely follow the GSA SmartPay requirements.</li> <li>• GSA SmartPay program provides procedures for processing travel card applications and training prior to using government purchase cards.</li> <li>• The card bears the employee's name and can be used only by that employee for official purchases in compliance with the agency's regulations and procedures and GSA Government Commercial Credit Card Services contract.</li> <li>• CFPB has a designated billing office that receives the "official invoice," and is responsible for ensuring payment of the official invoice in accordance with Prompt Payment Act deadlines.</li> <li>• CFPB organizational goals in this area are in line with the Treasury Financial Manual requirements.</li> </ul> | <p>Additional Action Suggested</p> <p>2012.TR.3 (Performance Improvement Opportunity): While the Policy On Travel Cards and Temporary Travel Duty is finalized and approved, the relocation expenses policy document is in an interim stage. We recommend that the Interim Relocation Expenses Policy and the rules governing such expenditure be finalized and approved.</p> |
| Management systems and risk management best practices          | <ul style="list-style-type: none"> <li>• Widely-used federal systems are leveraged to support the travel program.</li> <li>• Management systems are driven by Treasury BPD.</li> <li>• On-going post payment audits are performed on samples of Travel Vouchers.</li> <li>• CFPB management conducts employee satisfaction surveys to assess the travel policy and processes.</li> <li>• Internal controls on operations and financial reporting are designed and implemented to reduce reputational risk.</li> </ul>   | No recommendations provided for this performance audit element.   |

## Section 4: Budget

---

The Dodd-Frank Act provides the CFPB with a unique funding mechanism. The Act provides that the CFPB may receive an amount not to exceed a fixed percentage of the 2009 operating expenses of the Federal Reserve System, set at 10 % in FY2011, 11% in FY2012, and 12 % in FY2013 and thereafter, with adjustments for inflation. This funding is not subject to the traditional formulation and review of the Congressional appropriations process. Quarterly funding requests are prepared and presented to the Board of Governors of the Federal Reserve System. Receipt of funds from the Federal Reserve authorizes the agency's budget spending authority.

The CFPB Director is responsible for providing the Office of Management and Budget (OMB) with a report on financial operating plans and forecasts. Section 1017(a)(2) of the Dodd-Frank Act specifies the annual funding cap for the Bureau. Should the agency Director determine a need for appropriated funds, the Director shall prepare a report that illustrates how funding needs exceed the dollars transferred from the Federal Reserve. This dollar amount is capped at \$200 million per year for fiscal year (FY) 2010 through FY2014. Other than this funding, CFPB collects filing fees from developers under the Interstate Sales Full Disclosure Act (ILSA), which fees are applied towards the costs that the Bureau incurs for the ILS program operations. The Bureau is also authorized to collect civil penalties in any judicial or administrative action under the Federal consumer financial laws. These funds are available to the Bureau for payments to the victims of activities for which civil penalties have been imposed under the Federal consumer financial laws. To the extent that such victims cannot be located or such payments are otherwise not practicable, the Bureau may use such funds for the purpose of consumer education and financial literacy programs.

The purpose of this assessment is to evaluate the budget process and strategic use of the budget to achieve its mission and performance goals as well as to make recommendations for improving the effectiveness and efficiency of the organization.

### 4.1 Scope of Audit

The scope of this audit is defined by three key factors: (1) the set of Federal requirements and regulations in this area; (2) performance that CFPB has demonstrated to date and that represents the core of its current strategic planning, budgeting and performance measurement process; and (3) the future-state that CFPB has planned in this area, taking into account Federal standards and best practices. The scope of our evaluation includes:

- Alignment of strategic planning and budgeting, including the establishment of performance outcomes and performance measures that are aligned with budget formulation and monitoring;
- Budget formulation and execution methods, processes, and tools; and
- Budget office organization, staffing and capabilities.

During the FY12 performance audit, we reviewed documentation that already exists and is in operational use, as well as policies and plans that are being formulated to further define the strategic planning and budgeting process, resources, and assignments for the future. Specifically, we reviewed the following artifacts provided by CFPB:

- Memoranda issued by the Bureau's Legal Division outlining the applicability of Federal strategic planning, budgeting and performance planning requirements to the agency;

- Policies and Procedures documentation for planning, budget formulation, budget execution, recording of commitments and obligations, and performance reporting;
- Agreement and amendment to agreements of funding for CFPB;
- Funds transfer requests and acknowledgements;
- Strategic plans, budget documents and supporting divisional and program office budget data;
- Mission, goals and performance metrics used to measure and report performance;
- Government Performance and Results Modernization Act of 2010 (GPRMA) (Public Law 111-352) compliance strategy and planning documents;
- Budget formulation guidance documents, templates and standard forms;
- Reports issued by the Office of Chief Financial Officer (OCFO) that provide periodic budget and actual expenditure to assist monitoring and control processes;
- Internal quarterly performance reporting documents;
- Review of the financial audit report, and financial statements for FY11;
- Draft Government Accountability Office (GAO) engagement letter that outlines the scope of the FY12 external financial audit; and
- OCFO organization chart and budget responsibilities document.

Specifically, our audit included a review of the following components:

- Applicable language under Title X of the Dodd-Frank Act to identify applicable statutory requirements;
- Applicable language under GPRMA to better understand applicable statutory requirements;
- Strategic planning and internal and external performance reporting process, and its relationship to resources and cost allocation;
- Budget formulation process, including: (1) the parties involved; (2) the timing of activities; and (3) the methods and tools that are used;
- Budget execution process, including: (1) tracking of commitments and outlays; and (2) periodic reporting of budget execution and monitoring data;
- Transparency and information available to the public related to the strategic plan and budget;
- Major IT systems that are involved in the budget process;
- Current service agreements with U.S. Department of the Treasury – Bureau of Public Debt (BPD), Administrative Resource Center (ARC);
- Plans for verification and validation methods to be used for reporting performance;
- Staffing plan of the budget organization within CFPB;
- Assessment of work efforts that are being produced by CFPB’s contractors; and
- Consideration of any findings and recommendations arising from internal and external performance reviews or oversight efforts in this area.

In addition, we assessed the extent to which CFPB has addressed specific findings and recommendations from the FY11 performance audit within the Budget area.

## 4.2 Evaluation Criteria

The purpose of this section is to describe the evaluation criteria for this review area. As with other areas of performance, our audit focused on three sets of criteria: (1) compliance with legal requirements; (2) achievement of organizational goals; and (3) alignment with performance standards, best practices, and/or benchmarks.

### 4.2.1 Compliance with the Law

The ASR Team reviewed Title X of the Dodd-Frank Act to determine compliance with all applicable budgeting and funding sections of the law. The bullets below describe specific provisions of the Dodd-Frank Act that establish requirements and evaluation criteria in the Budget area.

- **Sections 1017(a)(1) and (3) of the Dodd-Frank Act** specify the process by which the Bureau requests funding from the Board of Governors based on amounts determined by the Director to be reasonably necessary to carry out the authorities of the Bureau.
- **Section 1017(a)(2) of the Dodd-Frank Act** specifies the annual funding cap for the Bureau—amounting to a fixed percentage of the 2009 operating budget of the Federal Reserve System, which is 10 percent of such expenses for FY11, 11 percent for FY12 and 12 percent for 2013 and thereafter with adjustments for inflation. Further, this section specifies that the funds derived from the Federal Reserve System shall not be subject to review by the Committees on Appropriations of the House of Representatives and the Senate.
- **Section 1017(a)(4) of the Dodd-Frank Act** requires CFPB to provide OMB with copies of the Bureau’s financial operating plans and forecasts as well as copies of the quarterly reports of the financial condition and results of operations of the Bureau. CFPB is required to prepare annual financial statements; implement and maintain financial management systems that comply substantially with Federal financial management system requirements and applicable Federal accounting standards; and provide to the Comptroller General of the United States an assertion as to the effectiveness of the internal controls that apply to financial reporting by the Bureau, using the standards established in section 3512(c) of title 31, United States Code. The CFPB financial statements shall not be consolidated with the financial statements of either the Board of Governors or the Federal Reserve System.
- **Section 1017(a)(5) of the Dodd-Frank Act** specifies the Comptroller General shall annually audit the financial transactions of the Bureau in accordance with Generally Accepted Government Auditing Standards (GAGAS), and submit to the Congress a report of each annual audit conducted under this subsection. A copy of each audit report shall also be furnished to the President and to the Bureau at the time submitted to the Congress.
- **Section 1017(b) of the Dodd-Frank Act** requires the Federal Reserve to establish a separate CFPB fund—maintained and established at a Federal Reserve bank—where all amounts transferred to the Bureau shall be deposited.

- **Section 1017(e) of the Dodd-Frank Act** authorizes the Bureau Director to determine whether the funds set aside from the Federal Reserve System are sufficient to carry out the authorities of the Bureau. If it is determined that the funds are insufficient, the Director shall prepare a report regarding the extent to which the funding needs are anticipated to exceed the funded amount. Based on this report, the Bureau may request appropriations up to \$200 million per year for FY12 through FY14.

The CFPB's Legal Division has determined that the Bureau is generally subject to the Government Performance and Results Act (GPRA) and GPRA-MA. However, it has also determined—based on Section 1017(a)(4)(E) of the Dodd-Frank Act—that the Bureau need not comply with those portions of GPRA or GPRA-MA that require an agency to follow OMB guidance or to otherwise submit to OMB jurisdiction or oversight. Recognizing these Legal Division determinations, we reviewed CFPB's strategic planning and performance measurement activities in relation to GPRA-MA requirements; including the following:

- Alignment of strategic plans with presidential terms of office;
- Establishment and achievement of any priority goals that align to government-wide performance plans;
- Establishment of a link between the performance goals in the annual plan with goals in the strategic plan;
- Description of the strategies and resources in the strategic plan;
- Description of a performance framework, governance structure and achievements to date; and
- Description of future plans for better connecting plans, programs, and performance outcome information.

GPRA-MA updated the nearly 20-year-old GPRA Act—resulting in a more defined performance framework, with better connection among plans, programs, and performance information. The original 1993 law required agencies to create multi-year strategic plans, annual performance plans, and annual performance reports. The new legislation revises agency strategic planning requirements by aligning the plan period with presidential terms of office, requiring greater cross-agency alignment of goals and programs, and providing a congressional consultation process in the development of the plans. GPRA-MA includes requirements for quarterly reviews and progress assessments of government-wide and agency-level priority goals. The new law also revises agency annual performance planning requirements by requiring a link between the performance goals in the performance plan with the goals in the strategic plan. The performance plan also must describe the strategies and resources that will be used, and must cover a 2-year, rather than a 1-year period for Federal priority goals aligned to the agency.

## 4.2.2 Achievement of Organizational Goals

In addition to supporting the legislative requirements under the Dodd-Frank Act and the GPRA-MA, we evaluated budget formulation and execution policies, procedures and practices supporting the following organizational goals:

- Is the budget structured in a comprehensive and useful manner to assist in the accomplishment of CFPB's mission and strategic goals included in its strategic plan?
- Is the budget formulated to reflect the plans and aspirations of CFPB's divisions?

- Are the strategic planning and budget processes forward-looking and sensitive to new requirements and improved practices?
- Is budget execution effectively communicated to appropriate parties within Bureau management and the public?
- Is the budget organization set up to effectively plan for meeting the goals and the workload?
- Do current budget formulation and execution tools and reporting methods effectively support the monitoring and control needs of the Bureau and its divisions and program offices?

### **4.2.3 Alignment with Performance Standards and Best Practices**

The CFPB is not required to comply with OMB Circulars and related guidance, but may, where appropriate, choose to align with these standards for improvement of its organization and operations. The underlying practices in the relevant Circulars pertaining to budgeting can, at a minimum, be viewed as leading Federal practices. With this in mind, the following standards were considered as best practices when formulating recommendations in the Budget area:

- OMB Circular A-11, “Preparation, Submission, and Execution of the Budget;”
- OMB Circular A-136, “Financial Reporting Requirements;” and
- OMB Circular A-123, “Management’s Responsibility for Internal Control.”

## **4.3 Findings and Recommendations (FY12 Audit)**

In this section, we present findings and recommendations related to CFPB’s budget, which describes the agency’s progress towards achieving legislative compliance, attaining organizational goals, and meeting performance standards. In general, we noted that CFPB had addressed all relevant budgeting requirements under Title X of the Dodd-Frank Act. CFPB has more-fully documented policies related to critical aspects of the Federal Reserve funding request and transfer process. For the FY12 Operations Plan, CFPB loaded its budget in its financial management system on a program office basis for enhanced execution and control, and has also expanded the amount of information available to the public such as operational plans, funding levels, expenditures, and financial performance management against Bureau priorities. We also noted that CFPB has positioned itself for compliance with the requirements under GPRA-MA. CFPB is well-underway with a strategic planning process to incorporate GPRA-MA requirements. CFPB recently posted a draft GPRA-MA Strategic Plan on its website for public comment.

Within this review area, we examined the Bureau’s performance with respect to 23 total performance elements. The audit team provided no recommendations or suggestions for 22 of the 23 performance elements (96%), indicating that there were no significant performance issues in these areas and no identified opportunities for improvement. The remaining performance element has been addressed through a performance improvement opportunity. We identified no significant performance issues.

### **4.3.1 Performance Improvement Opportunities**

Below, we present information an aspect of performance related to FY12 performance issues that we believe could be improved, but does not require corrective action. For this performance improvement

opportunity, we offer suggestions for future action, and we summarize the criteria on which this suggestion is based.

**2012.BUD.1 Guidance for Collecting, Validating and Reporting Performance Data to Program Offices.** In the Bureau’s most recent Budget Justification pertaining to verification and validation of performance data, the CFPB indicated it “will strive to ensure that the information reported in performance documents and the processes used to develop that information is complete and reliable.” In accordance with GPRA-MA, Section 1116, “Agency Performance Reporting,” we recommend that CFPB continue to develop detailed policies and procedures for collecting, validating and reporting performance data to provide guidance and establish uniform standards across the agency.

### **4.3.2 Summary of Demonstrated Performance**

Table 4 presents information on the Bureau’s demonstrated performance and achievements across all 23 performance elements that were audited during FY12 in this review area.

**Table 4: Summary of Demonstrated Performance**

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Improvement Opportunity                              |
|---|--|--|
| <b>Compliance with the Law</b>  |  |  |
| <p>DODD FRANK ACT<br/>SEC. 1017. FUNDING; PENALTIES AND FINES.<br/>(a) TRANSFER OF FUNDS FROM BOARD OF GOVERNORS.—<br/>(1) IN GENERAL.—Each year (or quarter of such year), beginning on the designated transfer date, and each quarter thereafter, the Board of Governors shall transfer to the Bureau from the combined earnings of the Federal Reserve System, the amount determined by the Director to be reasonably necessary to carry out the authorities of the Bureau under Federal consumer financial law, taking into account such other sums made available to the Bureau from the preceding year (or quarter of such year).</p>   | <ul style="list-style-type: none"> <li>• Documented budget funding process.</li> <li>• Interagency Agreement with Federal Reserve Board for Providing Funds.</li> <li>• Formal approved transfer requests and confirmation by the Board of Governors of the Federal Reserve Board to the Bureau Fund.</li> </ul>   | <p>No recommendations provided for this performance audit element.</p> |
| <p>(2) FUNDING CAP.—<br/>(A) IN GENERAL.—Notwithstanding paragraph (1), and in accordance with this paragraph, the amount that shall be transferred to the Bureau in each fiscal year shall not exceed a fixed percentage of the total operating expenses of the Federal Reserve System, as reported in the Annual Report, 2009, of the Board of Governors, equal to—<br/>    (i) 10 percent of such expenses in fiscal year 2011;<br/>    (ii) 11 percent of such expenses in fiscal year 2012;<br/>        and<br/>    (iii) 12 percent of such expenses in fiscal year 2013, and in each year thereafter.<br/>(B) ADJUSTMENT OF AMOUNT.—The dollar amount referred to in subparagraph (A) (iii) shall be adjusted H. R. 4173—601 annually, using the percent increase, if any, in the employment cost index for total compensation for State and local government workers published by the Federal Government, or the successor index thereto, for the 12-month period ending on September 30 of the year preceding the transfer.<br/>(C) REVIEWABILITY.—Notwithstanding any other provision in this title, the funds derived from the Federal Reserve System pursuant to this subsection shall not be subject to review by the Committees on Appropriations of the House of Representatives and the Senate.</p> | <ul style="list-style-type: none"> <li>• As of the end of the third quarter of FY12, the CFPB spent \$247 million, including commitments, obligations, and outlays against a budget of \$356 million for the fiscal year.</li> <li>• Funding provided for FY12 by transfers from the Federal Reserve reached \$343.3 million, approximately 63% against the ceiling of \$548 million. This ceiling represents 11% of the Federal Reserve’s 2009 operating budget.</li> <li>• CFPB’s budget justification for FY13 included in the President’s Budget is approximately \$448 million against a ceiling of \$598 million for the fiscal year.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |
| <p>(3) TRANSITION PERIOD.—Beginning on the date of enactment of this Act and until the designated transfer date, the Board of Governors shall transfer to the Bureau the amount estimated by the Secretary</p>  | <ul style="list-style-type: none"> <li>• Documented budget funding process.</li> <li>• Formal approved transfer requests.</li> </ul>   | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Improvement Opportunity                              |
|---|---|--|
| <p>needed to carry out the authorities granted to the Bureau under Federal consumer financial law, from the date of enactment of this Act until the designated transfer date.</p>   | <ul style="list-style-type: none"> <li>Budget execution tracking and status reporting.</li> </ul>   |  |
| <p>(4) BUDGET AND FINANCIAL MANAGEMENT.—</p> <p>(A) FINANCIAL OPERATING PLANS AND FORECASTS.—The Director shall provide to the Director of the Office of Management and Budget copies of the financial operating plans and forecasts of the Director, as prepared by the Director in the ordinary course of the operations of the Bureau, and copies of the quarterly reports of the financial condition and results of operations of the Bureau, as prepared by the Director in the ordinary course of the operations of the Bureau.</p> <p>(B) FINANCIAL STATEMENTS.—The Bureau shall prepare annually a statement of—</p> <p>(i) assets and liabilities and surplus or deficit;</p> <p>(ii) income and expenses; and</p> <p>(iii) sources and application of funds.</p> <p>(C) FINANCIAL MANAGEMENT SYSTEMS.— The Bureau shall implement and maintain financial management systems that comply substantially with Federal financial management systems requirements and applicable Federal accounting standards.</p> <p>(D) ASSERTION OF INTERNAL CONTROLS.— The Director shall provide to the Comptroller General of the United States an assertion as to the effectiveness of the internal controls that apply to financial reporting by the Bureau, using the standards established in section 3512(c) of title 31, United States Code.</p> <p>(E) RULE OF CONSTRUCTION.—This subsection may not be construed as implying any obligation on the part of the Director to consult with or obtain the consent or approval of the Director of the Office of Management and Budget with respect to any report, plan, forecast, or other information referred to in subparagraph (A) or any jurisdiction or oversight over the affairs or operations of the Bureau.</p> <p>(F) FINANCIAL STATEMENTS.—The financial statements of the Bureau shall not be consolidated with the financial statements of either the Board of Governors or the Federal Reserve System.</p> | <ul style="list-style-type: none"> <li>Quarterly budget execution reports provided to OMB.</li> <li>Quarterly financial statements for the first three quarters in FY12 have been sent to OMB in the month following the end of each quarter.</li> <li>FY11 annual financial statements were sent to OMB on November 15, 2011.</li> <li>The CFPB financial statements have never been consolidated with either the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve, or the Federal Reserve System.</li> <li>Implemented financial management system suite hosted by the U.S. Department of the Treasury Bureau of Public Debt (BPD) – Administrative Resource Center.</li> <li>CFPB hired an Internal Control Over Financial Reporting (ICFR) contractor to support the Internal Control Assurance.</li> <li>In accordance with FMFIA and the Dodd-Frank Act, CFPB provided Statement of Management Assurances, including Assertion of Financial Management Systems and Internal Controls for FY11.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |
| <p>(5) AUDIT OF THE BUREAU .— H. R. 4173—602</p>  | <ul style="list-style-type: none"> <li>GAO conducted an independent audit of CFPB financial</li> </ul>  | <p>No recommendations provided for</p>                                 |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Improvement Opportunity |
|---|--|---|
| <p>(A) IN GENERAL.—The Comptroller General shall annually audit the financial transactions of the Bureau in accordance with the United States generally accepted government auditing standards, as may be prescribed by the Comptroller General of the United States. The audit shall be conducted at the place or places where accounts of the Bureau are normally kept. The representatives of the Government Accountability Office shall have access to the personnel and to all books, accounts, documents, papers, records (including electronic records), reports, files, and all other papers, automated data, things, or property belonging to or under the control of or used or employed by the Bureau pertaining to its financial transactions and necessary to facilitate the audit, and such representatives shall be afforded full facilities for verifying transactions with the balances or securities held by depositories, fiscal agents, and custodians. All such books, accounts, documents, records, reports, files, papers, and property of the Bureau shall remain in possession and custody of the Bureau. The Comptroller General may obtain and duplicate any such books, accounts, documents, records, working papers, automated data and files, or other information relevant to such audit without cost to the Comptroller General, and the right of access of the Comptroller General to such information shall be enforceable pursuant to section 716(c) of title 31, United States Code.</p> <p>(B) REPORT.—The Comptroller General shall submit to the Congress a report of each annual audit conducted under this subsection. The report to the Congress shall set forth the scope of the audit and shall include the statement of assets and liabilities and surplus or deficit, the statement of income and expenses, the statement of sources and application of funds, and such comments and information as may be deemed necessary to inform Congress of the financial operations and condition of the Bureau, together with such recommendations with respect thereto as the Comptroller General may deem advisable. A copy of each report shall be furnished to the President and to the Bureau at the time submitted to the Congress.</p> <p>(C) ASSISTANCE AND COSTS.—For the purpose of conducting an audit under this subsection, the Comptroller General may, in the discretion of the Comptroller General, employ by contract,</p> | <p>statements for FY11 and submitted a report in accordance with requirements of the Dodd-Frank Act.</p> <ul style="list-style-type: none"> <li>• An engagement letter has been executed with the GAO to conduct an independent financial statement audit for CFPB for FY12.</li> <li>• The scope of the GAO engagement letter addresses the requirements of the legislation.</li> </ul> | <p>this performance audit element.</p>    |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Improvement Opportunity                              |
|---|---|--|
| <p>without regard to section 3709 of the Revised Statutes of the United States (41 U.S.C. 5), professional services of firms and organizations of certified public accountants for temporary periods or for special purposes. Upon the request of the Comptroller General, the Director of the Bureau shall transfer to the Government Accountability Office from funds available, the amount requested by the Comptroller General to cover the full costs of any audit and report conducted by the Comptroller General. The Comptroller General shall credit funds transferred to the account established for salaries and expenses of the Government Accountability Office, and such amount shall be available upon receipt and without fiscal year limitation to cover the full costs of the audit and report.</p>   |   |  |
| <p>(b) CONSUMER FINANCIAL PROTECTION FUND.— H. R. 4173—603<br/>                     (1) SEPARATE FUND IN FEDERAL RESERVE ESTABLISHED.— There is established in the Federal Reserve a separate fund, to be known as the “Bureau of Consumer Financial Protection Fund” (referred to in this section as the “Bureau Fund”). The Bureau Fund shall be maintained and established at a Federal reserve bank, in accordance with such requirements as the Board of Governors may impose.<br/>                     (2) FUND RECEIPTS.—All amounts transferred to the Bureau under subsection (a) shall be deposited into the Bureau Fund.</p>   | <ul style="list-style-type: none"> <li>• CFPB has documented the budget funding process.</li> <li>• Federal Reserve account services agreement is executed.</li> <li>• A separate fund has been established at the Federal Reserve for CFPB, and all amounts transferred by the Federal Reserve have been deposited into the separate CFPB fund.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |
| <p>(e) AUTHORIZATION OF APPROPRIATIONS; ANNUAL REPORT.—<br/>                     (1) DETERMINATION REGARDING NEED FOR APPROPRIATED FUNDS.—<br/>                     (A) IN GENERAL.—The Director is authorized to determine that sums available to the Bureau under this section will not be sufficient to carry out the authorities of the Bureau under Federal consumer financial law for the upcoming year.<br/>                     (B) REPORT REQUIRED.—When making a determination under subparagraph (A), the Director shall prepare a report regarding the funding of the Bureau, including the assets and liabilities of the Bureau, and the extent to which the funding needs of the Bureau are anticipated to exceed the level of the amount set forth in subsection (a)(2). The Director shall submit the report to the President and to the Committee on Appropriations of the Senate and the Committee on Appropriations of the House of Representatives.</p> | <ul style="list-style-type: none"> <li>• CFPB did not request an appropriation for FY11 and FY12.</li> <li>• An "Annual Report of the Consumer Financial Protection Bureau Pursuant to Section 1017(e)(4) of the Dodd-Frank Act" was submitted to Congress and posted on the CFPB website.</li> </ul>   | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance   | Recommendation or Improvement Opportunity                              |
|---|--|--|
| <p>(2) AUTHORIZATION OF APPROPRIATIONS.—If the Director makes the determination and submits the report pursuant to paragraph (1), there are hereby authorized to be appropriated to the Bureau, for the purposes of carrying out the authorities granted in Federal consumer financial law, \$200,000,000 for each of fiscal years 2010, 2011, 2012, 2013, and 2014.</p> <p>(3) APPORTIONMENT.—Notwithstanding any other provision of law, the amounts in paragraph (2) shall be subject to apportionment under section 1517 of title 31, United States Code, and restrictions that generally apply to the use of appropriated funds in title 31, United States Code, and other laws.</p> <p>(4) ANNUAL REPORT.—The Director shall prepare and submit a report, on an annual basis, to the Committee on Appropriations of the Senate and the Committee on Appropriations of the House of Representatives regarding the financial operating plans and forecasts of the Director, the financial condition and results of operations of the Bureau, and the sources and application of funds of the Bureau, including any funds appropriated in accordance with this subsection.</p> |  |  |
| <p>GPRA MODERNIZATION ACT OF 2010<br/>REVISED SEC. 306. CHAPTER 11 OF TITLE 31, USC</p> <p>(a) AGENCY STRATEGIC PLAN Not later than the first Monday in February of any year following the year in which the term of the President commences.<br/>Under section 101 of title 3, the head of each agency shall make available on the public website of the agency a strategic plan and notify the President and Congress of its availability. Such plan shall contain —</p> <p>(1) A comprehensive mission statement covering the major functions and operations of the agency;</p> <p>(2) General goals and objectives, including outcome-oriented goals, for the major functions and operations of the agency;</p> <p>(3) A description of how any goals and objectives contribute to the Federal Government priority goals required by section 1120(a) of title 31.</p>   | <ul style="list-style-type: none"> <li>• CFPB has drafted a 5-year Strategic Plan for the period FY13 to FY18.</li> <li>• The most recent version of the CFPB's draft Strategic Plan was posted to the CFPB's website for public comment on September 25, 2012.</li> <li>• The draft Strategic Plan documents 4 strategic goals, 11 desired outcomes in support of the goals, 25 strategies that state the actions CFPB will take to accomplish the outcomes, 27 performance measures to be tracked against specific targets in order to assess progress towards the outcomes, and 4 performance indicators to be tracked and used to assess progress towards the outcomes.</li> <li>• CFPB plans to invite public and Congressional comments over the next few months and make the final GPRA-MA strategic plan public in February 2013.</li> <li>• CFPB intends to publish its final Strategic Plan on the Bureau's website and notify both the President and Congress.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |
| <p>REVISED SEC. 1115 CHAPTER 11 OF TITLE 31, USC</p>  | <ul style="list-style-type: none"> <li>• CFPB has published the FY13 Budget Justification on its</li> </ul>  | <p>No recommendations provided for</p>                                 |

| Performance Requirement or Standard  | Demonstrated Performance   | Recommendation or Improvement Opportunity |
|--|--|---|
| <p>(b) AGENCY PERFORMANCE PLANS.—Not later than the first Monday in February of each year, the head of each agency shall make available on a public website of the agency, and notify the President and the Congress of its availability, a performance plan covering each program activity set forth in the budget of such agency. Such plan shall —</p> <ol style="list-style-type: none"> <li>(1) Establish performance goals to define the level of performance to be achieved during the year in which the plan is submitted and the next fiscal year;</li> <li>(2) Express such goals in an objective, quantifiable, and measurable form unless authorized to be in an alternative form under subsection (c);</li> <li>(3) Describe how the performance goals contribute to—“(A) the general goals and objectives established in the agency’s strategic plan required by section 306(a)(2) of title 5; and “(B) any of the Federal Government performance goals established in the Federal Government performance plan required by subsection (a)(1);</li> <li>(6) Establish a balanced set of performance indicators to be used in measuring or assessing progress toward each performance goal, including, as appropriate, customer service, efficiency, output, and outcome indicators;</li> <li>(7) Provide a basis for comparing actual program results with the established performance goals;</li> <li>(8) A description of how the agency will ensure the accuracy and reliability of the data used to measure progress towards its performance goals, including an identification of—             <ol style="list-style-type: none"> <li>(A) The means to be used to verify and validate measured values;</li> <li>(B) The sources for the data;</li> <li>(C) The level of accuracy required for the intended use of the data;</li> <li>(D) Any limitations to the data at the required level of accuracy; and</li> <li>(E) How the agency will compensate for such limitations if needed to reach the required level of accuracy.</li> </ol> </li> </ol> <p>(c) The performance plan required by section 1115(b) of title 31 shall be consistent with the agency’s strategic plan. A performance plan may not be submitted for a fiscal year not covered by a current strategic plan under this section.</p> | <p>website, which includes an Agency Performance Plan based on initial goals and performance measures developed in 2011 and prior to the 5 year Strategic Plan for FY13 to FY18, which is currently being finalized.</p> <ul style="list-style-type: none"> <li>• A comparable template is planned for future updates to the Agency Performance Plan. The current template is modeled after a comparable plan published by the U.S. Department of the Treasury.</li> <li>• In its draft Strategic Plan, CFPB provides the framework for its performance measures and performance indicators.</li> <li>• CFPB has begun to integrate planning, performance reporting and budgeting activities.</li> </ul> | <p>this performance audit element.</p>    |

| Performance Requirement or Standard  | Demonstrated Performance  | Recommendation or Improvement Opportunity  |
|--|---|--|
| <p>REVISED SEC. 1116 CHAPTER 11 OF TITLE 31, USC</p> <p>(a) The head of each agency shall make available on a public website of the agency and to the Office of Management and Budget an update on agency performance.</p> <p>(b)(1) Each update shall compare actual performance achieved with the performance goals established in the agency performance plan under section 1115(b) and shall occur no less than 150 days after the end of each fiscal year, with more frequent updates of actual performance on indicators that provide data of significant value to the Government, Congress, or program partners at a reasonable level of administrative burden.</p> | <ul style="list-style-type: none"> <li>• The Budget Justification document discusses the Bureau's plans to develop performance measures to track progress toward achieving strategic goals in FY12 and beyond.</li> <li>• For the future, CFPB plans to continue comparing actual performance achieved with the stated performance goals in the performance plan for FY13.</li> <li>• As part of the FY13-14 Budget Formulation process, CFPB captured division-level information, describing demonstrated performance relative to strategic goals.</li> <li>• With the full adoption of GPRA-MA, and publishing of the agency performance plan in February 2013, the subsequent annual performance report would not be due until February 2014 (150 days after the end of the fiscal year).</li> </ul> | <p>Additional Action Suggested</p> <p>2012.BUD.1 (Performance Improvement Opportunity): In accordance with GPRA-MA and to drive uniform standards applied across the Bureau ensuring accuracy and reliability of performance data, we recommend that policies and procedures be developed for collecting, validating and reporting performance data.</p> |
| <p>NEW SEC. 1122 CHAPTER 11 OF TITLE 31, USC</p> <p>(a) ESTABLISHMENT.—At each agency, the deputy head of agency, or equivalent, shall be the Chief Operating Officer of the agency.</p> <p>(b) FUNCTION.—Each Chief Operating Officer shall be responsible for improving the management and performance of the agency,</p>  | <ul style="list-style-type: none"> <li>• CFPB has appointed a Chief Operating Officer (COO), who is responsible for the management and performance of the organization.</li> <li>• The FY 2013 budget incorporates COO divisional costs as a separate division in the CFPB entity budget.</li> </ul>  | <p>No recommendations provided for this performance audit element.</p>   |
| <p>NEW SEC. 1123 CHAPTER 11 OF TITLE 31, USC</p> <p>(a) PERFORMANCE IMPROVEMENT OFFICERS.—</p> <p>(1) ESTABLISHMENT.—At each agency, the head of the agency, in consultation with the agency Chief Operating Officer, shall designate a senior executive of the agency as the agency Performance Improvement Officer.</p>  | <ul style="list-style-type: none"> <li>• CFPB has appointed a Chief Strategy Officer who is responsible for the performance management of the Bureau and is assisting with the development of the Strategic Plan.</li> </ul>  | <p>No recommendations provided for this performance audit element.</p>   |
| <p><b>Achievement of Organizational Goals</b></p>  |   |  |
| <p>Budget formulation and execution reflects the overall organizational strategy and performance, and supports the accomplishment of CFPB's mission and goals.</p>   | <ul style="list-style-type: none"> <li>• CFPB is in the process of finalizing an agency Strategic Plan, which has been posted for public comment.</li> <li>• The Chief Financial Officer (CFO) issued guidance for the preparation of the FY14 budget estimates, including a requirement to connect budget requests to the Bureau's strategic and performance goals.</li> <li>• Budget formulation is primarily done using detailed MS Excel spreadsheet templates.</li> <li>• In the FY13 Budget Justification, the agency reported budgeted resource estimates across 3 major categories: (1) Supervision, Enforcement and Fair Lending &amp; Equal</li> </ul>  | <p>No recommendations provided for this performance audit element.</p>   |

| Performance Requirement or Standard  | Demonstrated Performance  | Recommendation or Improvement Opportunity                              |
|--|---|--|
|  | <p>Employment Opportunity; (2) Consumer Education and Engagement / Consumer Response; and (3) Research, Markets and Regulation.</p>   |  |
| <p>Budget organization is set up to effectively meet the goals of CFPB.</p>  | <ul style="list-style-type: none"> <li>• CFO role and responsibilities have been defined.</li> <li>• Organization chart for the Office of the CFO (OCFO) has been finalized with 5 functional areas: (1) Governance and Compliance, (2) Travel and Relocation, (3) Internal Control, (4) Planning and Budget, and (5) Budget Execution and Financial Reporting.</li> <li>• Responsibilities matrix has been developed for the Budget and Planning Formulation team.</li> <li>• Budget for FY13 includes approved personnel strength.</li> <li>• There is potential to add budget staff in key departments, as deemed necessary.</li> </ul>  | <p>No recommendations provided for this performance audit element.</p> |
| <p>Budget is formulated in a structured, comprehensive and useful manner to support effective and efficient management of personnel and other resources.</p> | <ul style="list-style-type: none"> <li>• The COO and CFO oversee all activities related to the development and submission of the annual budget and performance plans, including the development, modification and execution of annual financial plans.</li> <li>• The CFO provided organizational communication and guidance to participants in the FY14 budget estimates and FY13 operating plan finalization process, with target dates for major milestones.</li> <li>• The OCFO's Budget Office forwards a data call to program offices requesting them to provide their Budget and Performance Plan requests for the budget, as well as for any proposed updates on the budget request from the previous year.</li> <li>• Using formats and templates provided by the OCFO, program offices fill out the requested information to justify their budget request. The justifications are sent to the OCFO for review.</li> <li>• Personnel budget is developed based upon approved positions for each division and office.</li> <li>• Non-personnel budgets are broken down by program offices within each division.</li> <li>• Funding requests identified in the budget estimates for FY13 and FY14 of \$500,000 or greater are planned to be reviewed by the Investment Review Board (IRB).</li> <li>• Agency investments exceeding \$500,000 in contractual</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Improvement Opportunity                              |
|---|---|--|
|   | <p>services or external costs for a single budget year (or exceeding \$2.5 million over 5 or more years) are subject to IRB in-take and review.</p> <ul style="list-style-type: none"> <li>• Program Offices plan to make presentations to the Office of the Director on their budget requests.</li> <li>• Additionally, after the close of the second quarter, OCFO conducts a mid-year review with each program office to assess the financial position of the organization.</li> </ul>   |  |
| <p>Budget execution provides effective control over funds, and timely information to program offices and divisions, and CFPB management and OMB for monitoring actual expenditure against budget.</p> | <ul style="list-style-type: none"> <li>• A policy for Recording Commitments and Obligations has been documented.</li> <li>• Commitments are controlled and funds are obligated prior to purchase. Each program office sends to the OCFO completed Budget Control Sheets for each obligation &gt;\$3,000.</li> <li>• After Budget and Planning team confirm funding availability, requisition is entered in PRISM and sent for approval in accordance with the standard operating procedure (SOP) for Budget Execution Requisition and Approval Process.</li> <li>• OCFO verifies proper approval and coding of each requisition before a commitment is set up.</li> <li>• Personnel budget and spending is broken down between salaries and benefits, and reported on a CFPB-wide basis.</li> <li>• Position headcount is provided for each of the divisions.</li> <li>• Non-personnel budget and spending is provided for each of the divisions.</li> <li>• Information is provided year-to-date and also projected for the fiscal year. Variances are calculated and reflected in the spreadsheet.</li> <li>• Monthly budget execution reports are prepared and distributed to divisions and program offices.</li> <li>• Monthly meetings with program offices discuss the actual versus plan and spending.</li> <li>• Performance against the financial plan is reviewed with the Director, Deputy Director, Chief of Staff, and Chief Strategy Officer (Performance Improvement Officer) during each division's performance review.</li> <li>• Quarterly financial statements and notes to the financial</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard  | Demonstrated Performance  | Recommendation or Improvement Opportunity                              |
|--|---|--|
|  | <p>statements have been prepared, and submitted to OMB in the month following the quarter end.</p> <ul style="list-style-type: none"> <li>For transparency purposes, a CFO Quarterly Update is posted on the CFPB website and provides information and insight on funds transferred from the Federal Reserve Board, expenditures, and analysis of expenditures by division and large obligations.</li> </ul>  |  |
| <p>Budget formulation and execution tools and automated methods effectively support the needs of CFPB, and assist in an efficient solution to meet CFPB requirements.</p>                    | <ul style="list-style-type: none"> <li>Budget formulation is primarily done on spreadsheets.</li> <li>The FY12 budget was loaded at the divisional level.</li> <li>CFPB uses the BPD Financial Management system for budget execution and commitment control.</li> </ul>  | <p>No recommendations provided for this performance audit element.</p> |
| <p>Periodic reviews and monitoring have been designed and implemented to ensure periodic status updates are available in relation to accomplishment of goals and performance assessment.</p> | <ul style="list-style-type: none"> <li>A standardized performance review template was prepared for implementation CFPB-wide starting during the 3rd Quarter of FY12.</li> <li>Divisions have started to implement the uniform review process.</li> <li>The review process integrates a large number of different management artifacts (e.g., tools; divisional budgets, strategies, risks and policy dashboards) into one synthesized perspective of accomplishments, challenges, and risks.</li> <li>The review template provides for analysis and status on objectives and related performance measures, outcomes, activities and risks.</li> </ul>           | <p>No recommendations provided for this performance audit element.</p> |
| <p>Policies and procedures are documented to provide guidance, a control environment, and uniformity of operations within CFPB.</p>  | <ul style="list-style-type: none"> <li>Interagency agreement between the Board of Governors of the Federal Reserve System and CFPB governs the process for transferring funds to the Bureau Fund Account.</li> <li>A CFPB Procedure for Transferring Funds has been documented.</li> <li>A Budget Formulation and Financial Operating Plan Policy has been documented.</li> <li>A Recording Commitments and Obligations Policy has been documented.</li> <li>SOPs for Budget Execution Requisition and Approval Process have been documented and are operational.</li> <li>The CFO provides guidance for preparation of budget and performance plan.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |

| Performance Requirement or Standard  | Demonstrated Performance   | Recommendation or Improvement Opportunity                       |
|--|--|---|
| <b>Alignment with Performance Standards and Best Practices</b>   |  |   |
| Strategic planning and performance management practices are in line with Federal standards and meet internal and external requirements | <p>Internal</p> <ul style="list-style-type: none"> <li>• CFPB has developed a standardized review procedure and templates for organizing information related to periodic planning and financial reviews.</li> <li>• The Office of Strategy has developed strategic planning and performance management process with CFPB-wide guidance and templates.</li> </ul> <p>Public-Facing</p> <ul style="list-style-type: none"> <li>• CFPB has communications and planning documentation related to its current GPRA-MA Strategic Plan development effort.</li> <li>• CFPB has developed a draft strategic plan, which incorporates GPRA-MA concepts outlining high-level organizational priorities, "outcome" objectives, annual performance management plans.</li> </ul>  | No recommendations provided for this performance audit element. |
| Budget is formulated to identify resource requirements at the program/cost center level  | <ul style="list-style-type: none"> <li>• Budget formulation for both personnel and non-personnel expenditures occur at the office level and rolls up to the divisional and entity level.</li> </ul>  | No recommendations provided for this performance audit element. |
| Fund management and reporting is executed to facilitate proper control over fund utilization   | <ul style="list-style-type: none"> <li>• A Recording Commitments and Obligations Policy has been documented.</li> <li>• Each program office sends to the OCFO completed Budget Control Sheets for each obligation &gt;\$3,000.</li> <li>• After Budget and Planning team confirm funding availability, requisition is entered in PRISM and sent for approval in accordance with the standard operating procedure (SOP) for Budget Execution Requisition and Approval Process.</li> <li>• OCFO verifies proper approval and coding of each requisition before a commitment is established.</li> <li>• Personnel budget and spending is broken down between salaries and benefits, and reported on a CFPB-wide basis.</li> <li>• Position headcount is provided for each of the divisions.</li> <li>• Non-personnel budget and spending is provided for each of the divisions.</li> <li>• Information is provided year-to-date and also projected for the fiscal year. Variances are calculated and reflected</li> </ul> | No recommendations provided for this performance audit element. |

| Performance Requirement or Standard   | Demonstrated Performance  | Recommendation or Improvement Opportunity                              |
|---|---|--|
|   | <p>in the spreadsheet.</p> <ul style="list-style-type: none"> <li>• Monthly meetings with program offices discuss the actual versus plan are working meetings.</li> <li>• Performance against the financial plan is reviewed with the Director, Deputy Director, Chief of Staff, and Chief Strategy Officer (Performance Improvement Officer) during each division’s periodic performance review.</li> <li>• Quarterly financial statements and notes to the financial statements have been prepared, and submitted to OMB in the month following the quarter end.</li> <li>• A CFO Quarterly Update is posted on the CFPB website and provides information and insight on funds received from the Federal Board, expenditures, and analysis of expenditures by division and large obligations.</li> </ul>          |  |
| <p>Proper internal control is operational around budget formulation and execution</p> | <ul style="list-style-type: none"> <li>• Quarterly budget execution reports provided to OMB.</li> <li>• Quarterly financial statements for the first three quarters have been sent to OMB in each of the month following the end of each quarter.</li> <li>• FY11 annual financial statements were sent to OMB on November 15, 2011.</li> <li>• Implemented financial management system suite hosted by the U.S. Department of the Treasury Bureau of Public Debt (BPD) – Administrative Resource Center.</li> <li>• CFPB hired an ICFR contractor to support the Internal Control Assurance.</li> <li>• In accordance with FMFIA and the Dodd-Frank Act, CFPB provided Statement of Management Assurances, including Assertion of Financial Management Systems and Internal Controls for FY11 and FY12.</li> </ul> | <p>No recommendations provided for this performance audit element.</p> |

## 4.4 Findings and Recommendations (FY11 Audit)

In FY11, the ASR Team conducted an initial evaluation of the CFPB's performance in the Budget area. Specifically, we examined the extent to which the Bureau had: (1) complied with relevant laws and regulations; (2) achieved organizational goals and objectives; and (3) aligned with industry best practices. Our analysis in FY11 was guided by the initial stages of organizational stand-up, compliance with Dodd Frank, and requirement to document policies related to critical aspects of the Board of Governors of the Federal Reserve funding request and transfer process. Last year, we understood Bureau-wide strategic plans were under development within CFPB. While that performance audit did not evaluate the progress or content of the draft plans, we encouraged CFPB to incorporate GPRA-MA concepts, outlining high-level organizational priorities, "outcome" objectives, and performance management plans.

Based on the analysis conducted in FY11, we offered recommendations and suggestions related to 7 performance elements in the Budget area. Included on this list was a broad spectrum of items, ranging from specific corrective actions to long-term strategic initiatives. The purpose of this FY12 performance audit follow-up is to: (1) evaluate the extent to which CFPB has addressed each of the suggestions and recommendations offered in FY11; and (2) provide new or updated recommendations for FY12, to address any residual performance gaps.

Based on the Bureau's demonstrated performance, we assigned a status of "Closed" to all 7 of the FY11 recommendations and suggestions (100%), indicating that no formal corrective action is required.

Table 5 presents the following information for each of the performance improvement opportunities contained in the FY11 report:

- **Recommendation Statement.** This column states the recommendation or suggestion that was provided in the FY11 Audit Report and provides a unique ID code for each.
- **Summary of CFPB Corrective Actions.** This column reports information about: (1) the actions that CFPB has taken to address the recommendation; (2) plans that CFPB has put in place to address the recommendation; and (3) the status of CFPB's efforts to address the recommendation.
- **FY12 Status.** This column reports the ASR Team's assessment of whether or not additional action is required to address the recommendation. A status of "no further action required" indicates that no further corrective action or monitoring is needed with respect to the recommendation—either because it has been achieved, or because the Bureau's ongoing operational and management activities provide adequate control over the recommended action.

**Table 5: Actions Taken by CFPB to Address Recommendations from the FY11 Audit Report**

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
| <p>CFPB should complete policy and procedural documentation. CFPB should continue its work underway to more-fully document policies related to critical aspects of the Federal Reserve funding request and transfer process. In addition, CFPB should continue to more-fully document policies related to budget formulation and execution / commitment control. Supplemental documentation should be developed to define detailed funding and budgetary procedures, roles and responsibilities, and performance management and monitoring practices. (2011.BUD.2.1)</p> | <ul style="list-style-type: none"> <li>• Interagency agreement with Federal Reserve System documents the transfer request process.</li> <li>• Procedures for transfer request have been developed and documented.</li> <li>• A process document has been developed, and provides information on authorization and timing of funding requests.</li> <li>• Other policies and procedures have been developed to define funding and budgetary procedures.</li> </ul>   | <p>Closed</p>                          |
| <p>CFPB should build a staffing plan for the budget organization. CFPB has been hiring additional budget staff over the past several months. As the bureau continues to expand its operations, we encourage the bureau to continue to reach out to other comparable U.S. federal agencies with unique funding mechanisms and missions similar to that of CFPB (e.g., FDIC and OCC) to garner ideas and recommendations for the structure and staffing levels of the budgeting operations. (2011.BUD.2.2)</p>   | <ul style="list-style-type: none"> <li>• CFO role and responsibilities have been defined.</li> <li>• Organization chart for the Office of the CFO has been finalized with 5 functional areas: 1) Governance and Compliance, 2) Travel and Relocation, 3) Internal Control, 4) Planning and Budget Formulation, and 5) Financial Management and Budget Execution.</li> <li>• Organization chart for the Budget and Planning organization is available.</li> <li>• Matrix of responsibilities has been developed.</li> <li>• Budget for FY13 includes approved FTE strength.</li> </ul> | <p>Closed</p>                          |
| <p>CFPB should continue to expand transparency of funding and expenditures. As the CFPB grows, we expect the bureau will continue to expand the amount of information available to the public (e.g., operational plans, funding levels, expenditures, financial performance management against bureau priorities, and the like). (2011.BUD.2.3)</p>  | <ul style="list-style-type: none"> <li>• CFPB has published FY13 Budget Justification.</li> <li>• Budget in Brief for FY12 and FY13 budgets has been published.</li> <li>• CFPB Congressional Justification for FY12 budget has been published.</li> <li>• CFO FY12 quarterly updates are published on the website.</li> <li>• CFPB Funding Requests and Confirmation letters received from FRB are published.</li> <li>• CFPB published a draft GPRA-MA Strategic Plan for FY13 to FY18 for comment.</li> </ul>  | <p>Closed</p>                          |
| <p>CFPB should increase automation of budget formulation and performance management. As is expected, much of CFPB's budget formulation process is manual and leverages spreadsheets – some of which are quite large and complex. CFPB should continue comparative analysis with other similar agencies to evaluate options for enhanced budget formulation and performance management automation. Where possible, we recommend leveraging pre-existing solutions to best serve the bureau at this stage of its evolution versus</p>                                      | <ul style="list-style-type: none"> <li>• Initial evaluation process of budget formulation and performance management tools used by other agencies has been completed.</li> <li>• Certain tools have been identified for detailed analysis and assessment.</li> <li>• Oracle Federal Financials and SharePoint, which are already being used by the Treasury BPD, are being considered to automate projections and data sharing.</li> </ul>  | <p>Closed</p>                          |

| FY11 Recommendation Statement (ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| <p>developing a bureau-specific solution. (2011.BUD.2.4)</p> <p>CFPB should continue to clarify and document the applicability of budget-related Circulars and Acts. CFPB continues its efforts to clarify and document the applicability to CFPB operations of various budgeting and performance management Circulars and Acts. CFPB has already adopted and will continue to integrate into its operations the principles and concepts contained within the relevant Circulars and Acts and the bureau will implement, where possible, best practice components. We support the bureau's plans to both document and implement all applicable standards and best practices. (2011.BUD.3.1)</p> | <ul style="list-style-type: none"> <li>• Legal Division has clarified applicability of the following in entirety or in part: CFO Act; GPRA and GPRA-MA; FMFIA; FFMIA; Reports Consolidation Act; Clinger Cohen Act; OMB Circulars, A-11, A-50, A-127, A-130, A-136 and A-123; and Treasury Financial Manual.</li> <li>• CFPB plans to implement applicable legal requirements.</li> </ul> | <p>Closed</p>                          |
| <p>CFPB should incorporate "outcome" objectives in strategic planning. We understand that bureau-wide strategic plans are under development within CFPB. While this performance audit did not evaluate the progress or content of the current draft plans, we encourage CFPB's progressive stages of strategic planning to incorporate GPRA-MA concepts outlining high-level organizational priorities, "outcome" objectives, annual performance management plans, relationship to funding and budgetary plans, progress review plans, accountability assignments, and plans for transparent monitoring and reporting. (2011.BUD.3.2)</p>   | <ul style="list-style-type: none"> <li>• CFPB developed and published, for comment, a draft GPRA-MA Strategic Plan for FY13 to FY18, which includes outcome objectives.</li> <li>• FY13 Budget Justification Section 3: Performance Plan and Report includes performance information under 8 preliminary performance indicators / measures.</li> </ul>                                    | <p>Closed</p>                          |
| <p>CFPB should load its budget at a divisional level. Starting with the FY 2013 President's Budget (currently being formulated) and the FY12 Operations Plan for CFPB, the bureau plans to construct its budget on a bottom-up basis by cost center. For the FY12 Operations Plan, CFPB plans to load its budget in its financial management system on a divisional basis for enhanced execution and control. We support the bureau's plan to begin loading the budget at a divisional level in FY12 for more effective management, control and accountability. (2011.BUD.3.3)</p>  | <ul style="list-style-type: none"> <li>• FY12 budget was loaded on a divisional basis in the financial accounting system.</li> <li>• FY14 Budget Estimates and FY13 Operating Plan are being prepared on a divisional basis.</li> </ul>   | <p>Closed</p>                          |

---

## Section 5: Communications and Transparency

---

### 5.1 Scope of Audit

In FY11, the ASR Team evaluated CFPB's performance in the area of Communications and Transparency. Specifically, we examined the extent to which the Bureau had: (1) complied with relevant laws and regulations; (2) achieved organizational goals and objectives; and (3) aligned with industry best practices. Our analysis in FY11 was guided by critical components found in successful communications plans used for building an organization strategy, including:

- **Determine Goals, Objectives and Strategies** – Determine the end state CFPB would like to reach with respect to communications and transparency initiatives and the strategies to achieve that goal;
- **Identify Audiences** – Identify the specific audiences CFPB wants to engage;
- **Establish Policies and Processes** – Make certain that there are internal policies and processes to ensure that CFPB's communications strategy can be properly executed;
- **Develop Key Messages** – Develop messages for key audiences, noting that while messages can be different, message consistency across the organization is important;
- **Identify Vehicles and Materials for Delivery** – Identify the vehicles and materials for message delivery that are appropriate for the targeted audiences and materials used; and
- **Define Metrics** – Define what success means and identify the metrics CFPB will use to determine how successful it has been in executing its communications strategy.

Our FY11 audit focused on major accomplishments and plans, including internal planning documents, memos and processes, media rollout plans, master outreach plans, reports, and media coverage. Based on the analysis conducted in FY11, we offered 43 recommendations and suggestions related to performance elements in the area of Communications and Transparency. Included on this list was a broad spectrum of items, ranging from specific corrective actions, to long-term strategic initiatives.

The purpose of this FY12 performance audit is to: (1) evaluate the extent to which CFPB has addressed each of the recommendations and suggestions offered in FY11; and (2) provide new or updated recommendations for FY12, to address any residual performance gaps. These "residual recommendations" have been grouped based on severity into one of the categories defined in Section 1.3.3.

### 5.2 Findings and Recommendations

Based on the Bureau's demonstrated performance, we assigned a status of "Closed" to all of the 43 FY11 recommendations and suggestions (100%), indicating that no formal corrective action is needed. Included among these closed items are 7 performance improvement opportunities, where suggestions are provided but no corrective action is required.

## 5.2.1 Summary of Demonstrated Performance

Table 6 presents the following information for each of the significant performance issues<sup>9</sup> and performance improvement opportunities contained in the FY11 report:

- **Recommendation Statement.** This column states the recommendation or suggestion that was provided in the FY11 Audit Report and provides a unique ID code for each.
- **Summary of CFPB Corrective Actions.** This column reports information about: (1) the actions that CFPB has taken to address the recommendation; (2) plans that CFPB has put in place to address the recommendation; and (3) the status of CFPB’s efforts to address the recommendation.
- **FY12 Status.** This column reports the ASR Team’s assessment of whether or not additional action is required to address the recommendation. A status of “no further action required” indicates that no further corrective action or monitoring is needed with respect to the recommendation—either because it has been achieved, or because the Bureau’s ongoing operational and management activities provide adequate control over the recommended action.

In this section, we identify residual recommendations and suggestions related to performance issues from FY11 that require further action. For each, we document: (1) the categorization of the residual performance issue based on its FY12 severity; (2) the criteria, condition, cause, and effect associated with the performance issue; and (3) our recommendations for addressing the performance issue.

## 5.2.2 Performance Improvement Opportunities

Below, we present information on aspects of performance related to performance issues that we believe could be improved, but do not require corrective action. For each of these performance improvement opportunities, we offer suggestions for future action, and we summarize the criteria on which these suggestions are based.

**2012.CT.1 FOIA Operations.** While significant progress has been made to operationalize Freedom of Information Act (FOIA) in-take, processing and reporting, we recommend the FOIA Office:

- a) Continue efforts to build an online “FOIA Reading Room” to provide public access to FOIA policies, procedures for initial requests and for appeals, logs, frequent requests, and performance reports; and
- b) Continue plans to further integrate the website FOIA request “in-take” functionality with the back-office eFOIA system (an automated application for processing FOIA and Privacy Act requests), in order to streamline and speed the FOIA request management process.

**2012.CT.2 Office of Consumer Education Mission and Vision Definition.** The Office of Consumer Engagement developed a plan in response to a recommendation in the FY11 Performance Audit to “continue to work on defining its own mission and vision” and “quickly move to fill out the

---

<sup>9</sup> The term “significant performance issue” includes (1) risks of deficiency or non-compliance; (2) deficiencies in internal controls; (3) noncompliance with provisions of laws, regulations, contracts, or grant agreements; (4) abuse; or (5) fraud.

office and develop the appropriate plans” to operate. Work efforts continue to fully implement the improvements outlined by the office. We recommend the office:

- a) Prioritize the remaining open positions for hiring, in accordance with the prioritized hiring plans of CFPB;
- b) Document and make available to all CFPB staff the Digital Media Team governance structure for the agency’s digital media channels; and
- c) Develop regular, repeatable performance measures for the efforts of the Digital Media Team.

**2012.CT.3 Agency-Wide Editorial Workflow.** In response to a recommendation made during the FY11 Performance Audit, an editorial workflow project had been conceptualized leveraging CFPB’s move to WordPress as the content management system for the agency’s primary website. However, the project has been delayed due to resource constraints. Given the significance of timely publication of research and educational materials, we recommend the Digital Media Team continue its plans to pilot and deploy the editorial workflow solution to speed the process for publishing content to the agency’s external website.

**2012.CT.4 Clearance 2.0.** While significant progress has been made to streamline the agency's process to clear and release materials to the public, we recommend the Office of the Executive Secretary:

- a) Continue its plans to implement a “Clearance 2.0” collaborative portal aimed to speed the release of materials; and
- b) Increase participation in government-wide forums of other agency Executive Secretaries to bring back, where applicable, best practices to the CFPB.

**2012.CT.5A Servicemembers Delayed Entry Program Training.** The Office of Servicemember Affairs developed a plan to respond to a recommendation in the FY11 Performance Audit to “continue its work with [the U.S. Department of Defense (DoD) to] move forward with beginning to revise new recruit curriculum.” The Office of Servicemember Affairs has moved forward with plans to procure services from industry to provide e-Learning and subject matter expert support focused on training military members in the Delayed Entry Program. We recommend the Office of Servicemember Affairs continue its planning efforts to build, test, and roll-out the financial education training program for military members in the Delayed Entry Program.

**2012.CT.5B Servicemembers Training Programs.** In May 2012, the Deputy Assistant Secretary of Defense (DASOD) and CFPB released a “Joint Statement of Principles on Consumer Financial Protection” to formalize the collaboration and cooperation between the DoD and the CFPB to help reduce consumer risk for servicemembers. We recommend the Office of Servicemember Affairs continue its dialogue with the DASOD to conceptualize and plan for the development of additional financial education training programs, focused on major life events pertaining to transitioning to and from military service.

**2012.CT.6 Multi-Lingual Communications.** With a focus for FY13 on multi-lingual print, video and social media communications, a website “translation project” is underway and led by the Office of Financial Education to provide more materials in Spanish via the CFPB’s website. We recommend

the Office of Financial Education continue its planning efforts to build, test, and publish the multi-lingual versions of financial literacy materials on the CFPB website.

**Table 6: Actions Taken by CFPB to Address Recommendations from the FY11 Audit Report**

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
| <p>The position of Ombudsman is mandated by the Dodd-Frank Act in the Office of External Affairs and its role within the organization is an important one. A detailee in this position could face some challenges in fulfilling a role that requires internal investigation given that employees could view him/her as temporary and be less than fully cooperative. Thus we recommend that the CFPB fill the position with a full-time employee as soon as possible. (2011.CT.1.1)</p> | <ul style="list-style-type: none"> <li>• While having served the agency since July 2011, Ms. Wendy Kamenshine was formally appointed as the Staff Director of the Office of the Ombudsman in May 6, 2012.</li> <li>• The Office of the Ombudsman explicitly reports directly into the CFPB's Office of the Director (i.e., not the Division of External Affairs) in order to promote the greatest degree of access and impartiality.</li> <li>• Currently, the Office of the Ombudsman is fully-staffed to approved levels.</li> <li>• An Office of Ombudsman Charter has been developed; an Ombudsman webpage has been built and linked from the main <a href="http://www.consumerfinance.gov">www.consumerfinance.gov</a> website bottom toolbar; and a public email inbox (<a href="mailto:cfpbombudsman@cfpb.gov">cfpbombudsman@cfpb.gov</a>), toll-free number, and fax number for the public to reach the Ombudsman's Office have all been established.</li> </ul> | <p>Closed</p>                          |
| <p>While the Consumer Advisory Board (CAB) has an important function within the organization and is mandated by the Dodd-Frank Act in External Affairs, by law the Board cannot be established until the Director of the CFPB is in place. Thus we recommend that preparations continue so the Board can be created as soon as possible following the approval of a Director. (2011.CT.1.2)</p>   | <ul style="list-style-type: none"> <li>• The CAB has been created within the approved organization structure of the Division of External Affairs.</li> <li>• In a press release dated August 28, 2012, Delicia Hand was formally announced as Staff Director of the CAB.</li> <li>• The CAB office is fully-staffed to approved levels, including a Policy Associate and Outreach Coordinator.</li> <li>• A press release announcing the appointment of 25 consumer experts to the CAB was made on September 12, 2012.</li> <li>• The CAB held its first meeting in St. Louis on September 27-28, 2012. A public calendar will be published along with corresponding meeting agendas.</li> </ul>   | <p>Closed</p>                          |
| <p>Designate a Private Education Loan Ombudsman by the date prescribed in Dodd-Frank. (2011.CT.1.3)</p>   | <ul style="list-style-type: none"> <li>• Internal CFPB approval for the Private Education Loan Ombudsman appointment was made on October 17, 2011.</li> <li>• Mr. Rohit Chopra currently serves as the designated Ombudsman.</li> <li>• The Private Education Loan Ombudsman office is fully-staffed to approved levels.</li> </ul>  | <p>Closed</p>                          |
| <p>While the CFPB has demonstrated that a great deal of thought has gone into its brand, one concern is that the CFPB defines its mission differently in different places. And while it's understandable to a degree that the CFPB would want to make its stated</p>  | <ul style="list-style-type: none"> <li>• CFPB's development and implementation of GPRA-MA provides the foundation for a unified articulation of the agency's mission, vision, values, strategy, outcome objectives, and key performance measures.</li> <li>• An internal wiki site has been deployed (CFPBedia) to generate additional reference material to promote more consistent communications and messaging.</li> </ul>  | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| <p>mission easy to understand, strict language guidelines pertaining to mandate, mission, and vision will help brand strength over time. Thus, we recommend the CFPB revisit the three areas it has publicly communicated in print its mandate, mission, vision and values and make efforts to reduce the variances and remain as consistent as possible across all mediums. (2011.CT.2.1)</p>   | <ul style="list-style-type: none"> <li>• "Plain language" and writing awareness, training and guidance is part of the new hire orientation curriculum.</li> <li>• External-facing electronic and print materials are designed with the "Plain Writing Act of 2010" in mind to promote clear and understandable communication to the public. The Director of Consumer Education and Engagement is the designated Plain Language official for CFPB.</li> <li>• A consumer-facing voice and tone guide has published for internal training and use across the agency.</li> </ul>                    |  |
| <p>The inclusion of the three criteria that pocketbook policy deliverables need to meet in order to maximize national and local attention is an excellent strategy. Also a recent op-ed articulating the impact of the 90/10 rule in the for-profit education sector on servicemembers is a good example of how to highlight the impact of certain policies on consumers. We recommend continuing to look for creative ways to help consumers express the challenges they face and their personal experiences. Doing this successfully will be central to the long-term success of the CFPB and will allow CFPB to develop fact-based ways to explain issues to other consumers. (2011.CT.2.2)</p> | <ul style="list-style-type: none"> <li>• CFPB attempts to profile real-life stories in its print materials and on the website and blog.</li> <li>• A social media campaign is underway leveraging real-life connections made by the Consumer Response team. CFPB has a presence on Facebook (with nearly 17,000 "likes"), Twitter and YouTube.</li> <li>• CFPB circulates a weekly e-mail to certain staff to communicate actual consumer issues that help to reinforce the agency's mission.</li> </ul>   | Closed                                 |
| <p>Given how significant the efforts have been to engage community groups, a tracker to organize the CFPB's efforts in this area will help it tell its story of who it is reaching and how it is reaching them. The tracker could include a list of groups the CFPB has</p>  | <ul style="list-style-type: none"> <li>• The CFPB Policy Committee (chaired by the CFPB Deputy Director) has documented plans to focus outreach field hearings with national and regional consumers, community groups, civil rights organizations, grass-roots advocacies, and other hard to reach audiences, in select cities not previously visited, and with topically-appropriate event agendas. Recent topics have principally centered on the mortgage markets.</li> <li>• The Division of External Affairs uses a variety of formats for its outreach efforts, including field</li> </ul> | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| <p>engaged, the last point of contact, nature of the contact, next steps to further engage the organization, and perhaps some assessment of the degree to which that organization is currently engaged. (2011.CT.3.1)</p>   | <p>hearings, round-table events, conferences, and webinars).</p> <ul style="list-style-type: none"> <li>• A spreadsheet is used to track and manage the outreach efforts. Contained in the spreadsheet are the event date, event format (e.g., field hearing, webinar, round-table event, conference), agenda, audience demographics, and registered attendees.</li> <li>• Matters of significance raised during outreach events (a.k.a., “read outs”) are logged in the spreadsheet for resolution. Formal consumer and community group comments and letters may also be initiated through the CFPB open rule-making process.</li> <li>• CFPB is in the process of procuring a more robust Customer Relationship Management (CRM) solution that it hopes to launch in FY13, with initial use by the Division of External Affairs. This CRM solution would facilitate retirement of the current tracking spreadsheet.</li> </ul>  |  |
| <p>The complete development of a searchable content resource will be a terrific way to share information and maximize bureau resources. (2011.CT.3.2)</p>   | <ul style="list-style-type: none"> <li>• To maximize CFPB resources, more information is being made available on the agency's website. Under the “Ask CFPB” menu of the agency's external website, a myriad of commonly asked questions are posted pertaining to credit cards, mortgages, student loans, and assistance for the elderly, servicemembers, and others.</li> <li>• Also on the website are industry reports, letters, bulletins and other materials to inform industry and the public.</li> <li>• A search feature is prominently displayed at the top of the website menu to ease user access to content within the website.</li> <li>• A Digital Media Team (chaired by the Acting Assistant Director of Consumer Education and Engagement) meets regularly to assess content presented within the agency's various digital media channels (including the website).</li> <li>• For internal materials, an internal wiki site has been deployed (CFPBedia) to generate additional reference material to promote more consistent communications and messaging.</li> <li>• Plans are underway to build a Content Library for use by agency staff, including studies from outside groups, think tanks and foundations as well as other CFPB-generated reports, projects, educational materials, brochures, field reports, and speeches.</li> </ul> | Closed                                 |
| <p>In our judgment, based on the information provided, the CFPB has met its obligations in this area. As mentioned in Table 18, while the role of the Ombudsman is filled with a detailee, it does not have a full-time permanent employee filling the position. We recommend doing so as soon as possible.</p> | <ul style="list-style-type: none"> <li>• Refer to comments in Item 2011.CT.1.1.</li> </ul>  | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations  |
|---|--|---|
| <p>(2011.CT.4.1)</p> <p>We recommend the CFPB continue its efforts around transparency and continue to find new ways to demonstrate its commitment in this area. Ideas include: making agendas and minutes from public and internal meetings available. (2011.CT.4.2)</p> | <ul style="list-style-type: none"> <li>• A FOIA Manager has been in place for over a year and manages the FOIA operations. Currently, the FOIA office is fully-staffed to approved levels.</li> <li>• FOIA requests can be submitted via e-mail, fax and normal mail. A “Public Guide to the FOIA Process” has been posted to the agency website in April 2012 and an eFOIA system was implemented in February 2012 tracking all FOIA requests.</li> <li>• With an eye toward sharing more publicly, the Office of the Executive Secretary facilitates the agency’s efforts to speed materials for release. CFPB has outlined the types of materials subject to the clearance process and those inherently open for release. For FY13, a collaborative internal portal implementation is being planned to further automate and streamline the clearance process.</li> <li>• Scheduled events for the CFPB Director and Deputy Director are made public and accessible on the agency website (under “Leadership calendar”). Meeting archives are also available for past Acting Directors.</li> <li>• The Division of External Affairs uses an e-mail distribution list of ~10,000 addresses (including national and regional consumers, community groups, civil rights organizations, grass-roots advocacies, members of Congress, members of the press corps, financial services firms, other industry firms) to proactively push same-day messages sharing remarks made by the CFPB Director and Deputy Director. These remarks are also posted on the agency website.</li> <li>• A tracking tool is used to inventory the CFPB’s Director’s and staff speaking requests.</li> <li>• A current version of the agency’s Unified Rule-Making Agenda was publicly-posted to the agency’s website on July 16, 2012. The current version is currently under review by the Office of Personnel Management.</li> <li>• A weekly e-mail is sent to all agency personnel to provide an update of upcoming meetings, events, reports, and the like.</li> <li>• A weekly post to the internal wiki website (CFPBedia) is used to distribute pertinent information to all agency staff.</li> <li>• A bi-monthly newsletter is distributed to all staff to update personnel on news, events, and personnel profiles.</li> </ul> | <p>Additional Action Suggested</p> <p>2012.CT.1 (Performance Improvement Opportunity): While significant progress has been made to operationalize Freedom of Information Act (FOIA) in-take, processing and reporting, we recommend the FOIA Office:</p> <ul style="list-style-type: none"> <li>a) Continue efforts to build an online “FOIA Reading Room” to provide public access to FOIA policies, procedures for initial requests and for appeals, logs, frequent requests, and performance reports; and</li> <li>b) Continue plans to further integrate the website FOIA request “in-take” functionality with the back-office eFOIA system (an automated application for processing FOIA and Privacy Act requests), in order to streamline and speed the FOIA request management process.</li> </ul> |
| <p>Consumer Engagement should continue to work on defining its own mission and vision, ensuring that they are in agreement with the mission and vision of the CFPB as a whole.</p>  | <ul style="list-style-type: none"> <li>• Aligned with the overall CFPB mission, the Office of Consumer Engagement has developed and published a mission and vision statement and posted it to the internal wiki site (CFPBedia). Along with the other offices within the Division of Consumer Education and Engagement, the Office of Consumer Engagement engaged in role chartering to identify areas of overlap and gaps in</li> </ul>   | <p>Additional Action Suggested</p> <p>2012.CT.2 (Performance Improvement Opportunity): We recommend the Office of</p>   |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations   |
|---|---|--|
| <p>Developing specific objectives for each office within the CFPB makes sense, but it is very important that those objectives align with the overall mission of the CFPB. (2011.CT.5.1)</p>   | <p>coverage in the Division of Consumer Education and Engagement mission.</p> <ul style="list-style-type: none"> <li>Recognizing the unique partnership between the Office of Consumer Education and the Office of Technology &amp; Innovation, the teams jointly developed (under the leadership of the Digital Media Team) a cross-functional governance structure to define roles and responsibilities between the two teams as it relates to the CFPB's digital media channels.</li> <li>A procurement package was released in the summer 2012 to acquire contractor management consulting services to continue refining the structure, operations and processes within the Office of Consumer Engagement. Work is planned to commence in fall 2012.</li> </ul> | <p>Consumer Education and Engagement:</p> <ul style="list-style-type: none"> <li>a) Prioritize the remaining open positions for hiring, in accordance with the prioritized hiring plans of CFPB;</li> <li>b) Document and make available to all CFPB staff the Digital Media Team governance structure for the agency's digital media channels; and</li> <li>c) Develop regular, repeatable performance measures for the efforts of the Digital Media Team.</li> </ul> |
| <p>Consumer Engagement should move quickly to fill out its office and develop the appropriate plans and policies to allow it to effectively operate. (2011.CT.5.2)</p>  | <ul style="list-style-type: none"> <li>The CFPB Chief Human Capital Officer has approved an office headcount of 10. Staffing efforts continue with prioritized hiring.</li> <li>Consumer Engagement has developed an organization chart, position descriptions, and promotion ladder.</li> </ul>  | <p>Closed</p>  |
| <p>We recommend Consumer Engagement continue to work the technology and information offices within CFPB to develop the scope, requirements and timeline of the project. (2011.CT.5.3)</p>   | <ul style="list-style-type: none"> <li>An editorial workflow project has been conceptualized following the agency's move to WordPress as the content management system for www.consumerfinance.gov. However, the project has been delayed due to resource constraints.</li> <li>Within the Digital Media Team's "product roadmap" for the website, plans are underway to pilot a version of editorial workflow in the Division of External Affairs starting in fall 2012.</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.CT.3 (Performance Improvement Opportunity): Given the significance of timely publication of research and educational materials, we recommend the Digital Media Team continue its plans to pilot and deploy the editorial workflow solution to speed the process for publishing content to the agency's external website.</p>  |
| <p>If it is determined that the Clearance Process is in need of improvement, we recommend considerations for a more streamlined approach and strongly encourage Consumer Engagement to be involved in the process of developing a new</p> | <ul style="list-style-type: none"> <li>With an eye toward sharing more publicly, the Office to the Executive Secretary facilitates the agency's efforts to speed materials for release.</li> <li>CFPB has outlined the types of materials subject to the clearance process and those inherently open for release. For FY13, a collaborative internal portal implementation is being planned to further automate and streamline the clearance process.</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.CT.4 (Performance Improvement Opportunity): While significant progress has been made to streamline the agency's process to clear and release materials to the</p>   |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations  |
|---|---|---|
| policy. (2011.CT.5.4)   |   | public, we recommend the Office of the Executive Secretary:<br><br>a) Continue its plans to implement a "Clearance 2.0" collaborative portal aimed to speed the release of materials; and<br><br>b) Increase participation in government-wide forums of other agency Executive Secretaries to bring back, where applicable, best practices to the CFPB. |
| We recommend Consumer Engagement continue to plan for the promotion of education content to ensure promotion is as seamless as possible once it is ready for publication. (2011.CT.5.5) | <ul style="list-style-type: none"> <li>• Under the "Ask CFPB" menu of the agency's external website, a myriad of commonly asked questions are posted pertaining to credit cards, mortgages, student loans, and assistance for the elderly, servicemembers, and others.</li> <li>• Also on the website are industry reports, letters, bulletins and other materials to inform industry and the public.</li> <li>• A search feature is prominently displayed at the top of the website menu to ease user access to content within the website.</li> <li>• A Digital Media Team (chaired by the Acting Assistant Director of Consumer Education and Engagement) meets regularly to assess content presented within the agency's various digital media channels (including the website).</li> <li>• Plans are underway to pilot a version of editorial workflow in the Division of External Affairs starting in fall 2012.</li> </ul> | Closed  |
| We recommend CFPB move forward with plans for the consumer experience blueprint for delivery in December 2011. (2011.CT.5.6)  | <ul style="list-style-type: none"> <li>• Plans have been created to guide the education and awareness training initiatives of the agency. Approved by the CFPB Policy Committee, these plans are structured into modules for targeted consumer education via the internet.</li> <li>• Module 1 (Paying for College) was accessed by over 89,000 users with thousands of feedback comments for continuous improvement to the module. A final build and national launch of Module 1 is planned for the fall 2012.</li> <li>• Module 2 (Owning a Home) has been approved by the Policy Committee to enter the concept phase to kick-off in fall 2012.</li> </ul>   | Closed  |
| We encourage CFPB to continue to use live   | <ul style="list-style-type: none"> <li>• CFPB is using live streaming to simulcast major agency events approximately twice each month.</li> </ul>   | Closed  |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| streaming as a communications tool, as it allows those who are unable to attend CFPB events the opportunity to be a part of them. (2011.CT.5.7)   | <p>Video content is available via the CFPB website both live and with playback features.</p> <ul style="list-style-type: none"> <li>• CFPB is also using comparable video streaming tools to provide information internal to the agency as part of quarterly all-hands meetings.</li> <li>• The CIO of CFPB reports plans to continue and expand the use of interactive and on-demand services via the agency's website.</li> </ul>   |  |
| We recommend the CFPB revisit the three areas it has publicly communicated in print (mission, vision and values) and make efforts to reduce the variances and remain as consistent as possible across all mediums. (2011.CT.7.1A)   | <ul style="list-style-type: none"> <li>• Refer to comments in Item 2011.CT.2.1.</li> </ul>  | Closed                                 |
| Specifically, discontinue using the "Mission" language as it's duplicative of the Statutory Purpose and Objectives (both of which use language that is clear and suitable for consumer facing communication), keep the vision and use it as a part of the language on the website and in consumer facing vehicles as part of a section devoted to "what does this mean for you". (2011.CT.7.1B) | <ul style="list-style-type: none"> <li>• CFPB's development and implementation of GPRA-MA provides the foundation for a unified articulation of the agency's mission, vision, values, strategy, outcome objectives, and key performance measures.</li> <li>• The CFPB mission, in print and as articulated within the GPRA-MA materials, has been purposefully shortened for ease of use. The articulated goals and outcomes of the GPRA-MA materials, along with the shortened mission, have been designed to align with the Statutory Purpose and Objectives.</li> <li>• To confirm this alignment, CFPB plans to submit its GPRA-MA plans for Congressional review in fall 2012.</li> <li>• An internal wiki site has been deployed (CFPBedia) to generate additional reference material to promote more consistent communications and messaging.</li> </ul> | Closed                                 |
| We recommend the CFPB continue to find ways to highlight other faces within the bureau as it grows and matures. (2011.CT.7.2)   | <ul style="list-style-type: none"> <li>• CFPB attempts to profile real-life stories in its print materials and on the website and blog.</li> <li>• A social media campaign is underway leveraging real-life connections made by the Consumer Response team. CFPB has a presence on Facebook (with nearly 17,000 "likes"), Twitter and YouTube.</li> <li>• CFPB circulates a weekly e-mail to certain staff to communicate actual consumer issues that help to reinforce the agency's mission.</li> </ul>  | Closed                                 |
| Given how significant the efforts have been to engage community groups, a tracker to organize the CFPB's efforts in this area will help it tell its story of who it's reaching and  | <ul style="list-style-type: none"> <li>• Refer to comments in Item 2011.CT.3.1.</li> </ul>  | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| <p>how it's reaching them. The tracker could include a list of groups the CFPB has engaged, the last point of contact, nature of the contact, next steps to further engaging the organization and perhaps some assessment of the degree to which that organization is currently engaged. (2011.CT.7.3)</p>   |  |  |
| <p>The complete development of a searchable content resource will be a terrific way to share information and maximize bureau resources. (2011.CT.7.4)</p>  | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.3.2.</li> </ul> | <p>Closed</p>                          |
| <p>The position of Ombudsman is mandated by the Dodd-Frank Act in External Affairs and its role within the organization is an important one. Further, a detailee in this position could face some challenges in fulfilling a role that requires internal investigation given that employees could view him/her as temporary and be less than fully cooperative. Thus we recommend that the CFPB fill the position with a full-time employee as soon as possible. (2011.CT.7.5)</p> | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.1.1.</li> </ul> | <p>Closed</p>                          |
| <p>While the Consumer Advisory Board has an important function within the organization and is mandated by the Dodd-Frank Act in external affairs, by law, the Board cannot be created until the Director of the CFPB is in place. Thus we recommend the Board be created as soon as possible following the approval</p>  | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.1.2.</li> </ul> | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
| of a Director. (2011.CT.7.6)  |  |  |
| We recommend that the CFPB continue working toward this being a fully-functional office. (2011.CT.7.7)  | <ul style="list-style-type: none"> <li>Ms. Camille Busette was appointed as the Assistant Director for the Office of Financial Education in November 2011.</li> <li>The Office of Financial Education is approved for staffing of 14 personnel and is currently staffed at 10, with additional requisitions posted. The Office of Financial Education is currently approved for a staffing level of 16 for FY13.</li> <li>Each quarter, to assess and manage performance, the Office of Financial Education contributes content to the Division of Consumer Education and Engagement Quarterly Performance Report scorecard.</li> </ul>  | Closed                                 |
| Identify ways to share with other agencies and make public how the CFPB has gone about its FOIA process. This is an area CFPB can exhibit some thought leadership. (2011.CT.7.8)  | <ul style="list-style-type: none"> <li>The CFPB FOIA Office has shared its eFOIA and eDiscovery implementation experiences with the US Department of Homeland Security for its consideration.</li> <li>Since the Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency and Export-Import Bank are using the same eFOIA tool as CFPB, an informal "Financial Sector FOIA Working Group" has been convened involving these agencies. FDIC is taking a lead to help gather the group about every quarter. An initial meeting will be held in the fall 2012.</li> <li>The working group plans to share experiences, thoughts and "best practices" examples.</li> </ul> | Closed                                 |
| Consumer Engagement should continue to work on defining its own mission and vision, ensuring that they are in agreement with the mission and vision of the CFPB as a whole. Developing a coordinated mission and vision will strengthen the CFPB brand over time. (2011.CT.7.9) | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.1.</li> </ul>   | Closed                                 |
| Consumer Engagement should move quickly to fill the office and develop the appropriate plans and policies to allow it to effectively operate. (2011.CT.7.10)  | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.2.</li> </ul>   | Closed                                 |
| We recommend Consumer Engagement continue to work with the technology and information offices within CFPB to develop the score, requirements and timeline of the  | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.3.</li> </ul>   | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| project. (2011.CT.7.11)  |  |  |
| If it is determined that the Clearance Process is in need of improvement, we recommend considerations for a more streamlined approach to the process and strongly encourage Consumer Engagement to be involved in the process of developing a new policy. (2011.CT.7.12) | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.4.</li> </ul>   | Closed                                 |
| We recommend Consumer Engagement continue to plan for the promotion of education content to ensure promotion is as seamless as possible once it is ready for publication. (2011.CT.7.13)   | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.5.</li> </ul>   | Closed                                 |
| We recommend CFPB continue to move forward with the consumer experience blueprint so that work that is dependent on it can move forward. (2011.CT.7.14)  | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.6.</li> </ul>   | Closed                                 |
| We encourage CFPB to continue to use live streaming as a communications tool, as it allows those who are unable to attend CFPB events the opportunity to be a part of them. (2011.CT.7.15)   | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.CT.5.7.</li> </ul>   | Closed                                 |
| We recommend the CFPB continue the planning process already underway for the convening event. (2011.CT.7.16)   | <ul style="list-style-type: none"> <li>An analysis of Federal Register submissions was performed. The Financial Fitness Forum event format was determined and a participant listing was compiled. Keynote speaker and moderator invitations were sent.</li> <li>The Financial Fitness Forum was held in December 2012 with approximately 200 attendees, including representatives from banking institutions, credit unions, industry trade associations, and other special interest groups.</li> <li>A draft whitepaper has been produced, focused on servicemembers in the Delayed Entry Program. The whitepaper summarizes the event with a detachable reference tear sheet for use</li> </ul> | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations   |
|---|--|--|
| <p>We recommend the CFPB continue to move forward with planning visits to the remaining military basic training sites in order to reach its goal of going to all military division basic training sites by January 2012. (2011.CT.7.17)</p> | <p>by young servicemembers. The whitepaper is expected to be published by early FY13.</p> <ul style="list-style-type: none"> <li>The Office of Servicemember Affairs is routinely meeting with the Deputy Assistant Secretary of Defense (DASOD), Military Community and Family Policy. This office within the DASOD owns the Personal Financial Readiness Program for the U.S. Department of Defense (DoD).</li> <li>In May 2012, the DASOD and CFPB released a Joint Statement of Principles on Consumer Financial Protection to memorialize the collaboration and cooperation between DOD and the CFPB to help reduce consumer risk for servicemembers.</li> <li>A significant number of visits have been made to U.S. Army, U.S. and U.S. Marine Corps sites. Emphasis is being placed on servicemembers in the Delayed Entry Program, targeting financial awareness training for those transiting into military service.</li> </ul> | <p>Closed</p>  |
| <p>We recommend the CFPB continue its work with DoD and move forward with revising new recruit curriculum. (2011.CT.7.18)</p>   | <ul style="list-style-type: none"> <li>CFPB developed a statement of work and received Investment Review Board (IRB) approval to procure services from industry to provide e-Learning and subject matter expert support focused on training military members in the Delayed Entry Program.</li> <li>The procurement package is currently pending release by the CFPB Office of Procurement. It is anticipated that training will require approximately 12 months to develop and prepare for full roll-out. The Office of Servicemember Affairs anticipates full DoD availability to use the training program by the start by October 2013.</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.CT.5A (Performance Improvement Opportunity): We recommend the Office of Servicemember Affairs continue its planning efforts to build, test, and roll-out the financial education training program for military members in the Delayed Entry Program.</p> <p>2012.CT.5B (Performance Improvement Opportunity): We recommend the Office of Servicemember Affairs continue its dialogue with the DASOD to conceptualize and plan for the development of additional financial education training programs, focused on major life events pertaining to transitioning to and from military service.</p> |
| <p>Adding additional languages to the website and generating select materials in other languages will allow the CFPB to engage consumers in populations it can only reach indirectly at this point in time. (2011.CT.8.1)</p>               | <ul style="list-style-type: none"> <li>The Office of Financial Education within the Division of Consumer Education and Engagement regularly procures translation services providing print materials in approximately 10 languages. An agency-wide Blanket Purchase Agreement is in place to support these efforts.</li> <li>The Office of Consumer Response leverages a separate translation services contract in carrying out its mission, supporting over 185 languages.</li> <li>With a focus for FY13 on multi-lingual print, video and social media communications, a website</li> </ul>  | <p>Additional Action Suggested</p> <p>2012.CT.6 (Performance Improvement Opportunity): We recommend the Office of Financial Education continue its planning efforts to build, test, and publish the multi-lingual versions of financial literacy materials</p>   |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
|  | <p>"translation project" is underway and led by the Office of Financial Education to provide more materials in Spanish via the CFPB's website.</p> <ul style="list-style-type: none"> <li>An informal, internal multi-lingual "working group" has also been established so assist with the language translation needs of the agency.</li> </ul>   | on the CFPB website.                   |
| <p>The Intergov office was recently staffed, and will be responsible for developing relationships with state, local and international officials. Full functionality of this office will further enhance the CFPB's ability to demonstrate its support and impact and also to solicit information at the state and local level. (2011.CT.8.2)</p> | <ul style="list-style-type: none"> <li>The Office of Intergovernmental Affairs (IGA) hired staff responsible for state and local engagement. Staff is also being hired for international engagement.</li> <li>IGA developed state-level initiatives, including state stakeholder meetings, state legislative tracking, and Director interaction with state attorneys general.</li> <li>IGA developed local initiatives, including local stakeholder meetings, cities events and Director interaction with mayors.</li> <li>IGA developed international initiatives, including international stakeholder meetings and steering of the U.S. delegation position on international negotiation regarding arbitration.</li> <li>IGA presented weekly activity summaries to the CFPB Director's Chief of Staff.</li> </ul>  | Closed                                 |
| <p>We recommend more documented planning so that the CFPB can outline key target groups and assess those relationships, and so that other departments within the CFPB can leverage third party traction/awareness. (2011.CT.8.3)</p>   | <ul style="list-style-type: none"> <li>The Division of External Affairs collaborates with other CFPB offices (including the offices of Enforcement, Supervision, Fair Lending &amp; Equal Opportunity, Financial Education, Financial Empowerment, Older Americans, Students, Servicemembers, Technology &amp; Innovation, and Minority &amp; Women Inclusion) to coordinate outreach efforts.</li> <li>The Division of External Affairs has created a comprehensive outreach plan that spans the nation and includes consumer protection, underserved, low-income, faith-based, and other nonprofit stakeholder constituencies. Included in this plan is the identification of a core of key national stakeholder groups to connect Community Affairs with local chapters of national organizations across the country.</li> <li>CFPB is in the process of procuring a more robust CRM solution it hopes to launch in FY13, with initial use by the Division of External Affairs. This CRM solution would facilitate retirement of the current "Community Affairs Tracker" spreadsheet.</li> </ul> | Closed                                 |
| <p>While thoughtful consideration of the CFPB's value proposition for consumers is worthwhile, the CFPB should develop a message architecture that considers the specific needs of all of its audiences (consumers, industry, policymakers, etc.). (2011.CT.10.1)</p>  | <ul style="list-style-type: none"> <li>The Division of External Affairs helps to tailor messages to the specific needs of all audiences—and to coordinate the strategic timing of press releases, consumer and industry rollouts, intergovernmental and legislative rollouts, Director's announcements, and outreach events in the field.</li> <li>Outside-the-Beltway events highlighting key CFPB policy deliverables in Minneapolis, Cleveland, Birmingham, New York, Sioux Falls, Tampa [cancelled due to weather emergency], and Detroit. Events included public town halls and field hearings featuring panels, public testimony, and roundtables with key stakeholders (including consumer and civil rights organizations, credit unions</li> </ul>  | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
| <p>As the organization matures and the staff grows, CFPB should strive to increase the frequency of blog posts (currently about one per week), in order to make this a more robust communications tool. (2011.CT.11.1)</p>   | <p>and community banks, members of Congress, and state and local officials).</p> <ul style="list-style-type: none"> <li>• A Division of External Affairs newsletter is sent to over 10,000 stakeholders twice monthly.</li> <li>• Blog posts on the CFPB website have increased as the organization has grown. CFPB has also expanded its use of other social media tools, including Facebook, Twitter, YouTube and broadcast e-mail.</li> <li>• Plans have been developed to guide education and awareness training initiatives of the agency, including the use of various digital media channels.</li> <li>• In addition to expanded use of the blog posts, the blueprint outlines use of paid advertising, public service announcements and other possible awareness campaigns – all in an attempt to position the CFPB as a resource for consumers and consumer advisors earlier, as individuals make major life decisions (e.g., Paying for College, Buying a Home).</li> </ul> | <p>Closed</p>                          |
| <p>To date there has been limited use of Webinars and Livestream, but the CFPB has honored its commitment to use them as a way of communications with the general public or allowing them to participate in an event. As the staff grows and CFPB hosts/participates in more events, this might become a more robust communications tool. (2011.CT.11.2)</p> | <ul style="list-style-type: none"> <li>• Refer to comments in Item 2011.CT.5.7.</li> </ul>  | <p>Closed</p>                          |
| <p>As additional staff is added, devoting time and resources to define success and establish metrics will allow the CFPB to evaluate itself and for others outside the CFPB to do the same. Also, as the staff will inevitably experience some turnover, having documented metrics for assessing performance is important. (2011.CT.12.1)</p>                | <ul style="list-style-type: none"> <li>• The Office of Media Relations defined metrics for success, including increasing press output and press hits, highlighting policy deliverables through high-impact events and rollouts, onboarding additional spokespeople, developing office infrastructure, and overall creation of a positive narrative around the CFPB's first year.</li> </ul>   | <p>Closed</p>                          |
| <p>Making the public aware of the CFPB is a sizeable task and thus, it has just begun to scratch the surface in this area. We do not have any recommendations at this time</p>   | <ul style="list-style-type: none"> <li>• Refer to comments in Items 2011.CT.5.6 and 2011.CT.11.1.</li> </ul>  | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions | FY12 Status / Residual Recommendations |
|---|-------------------------|--|
| beyond what the CFPB is already doing in this area. However, the CFPB should consider making public the many ways it tries to reach the public and ask for new ways it should consider via the website, social media, etc. (2011.CT.12.2) |                         |  |

## Section 6: Consumer Response

---

### 6.1 Scope of Audit

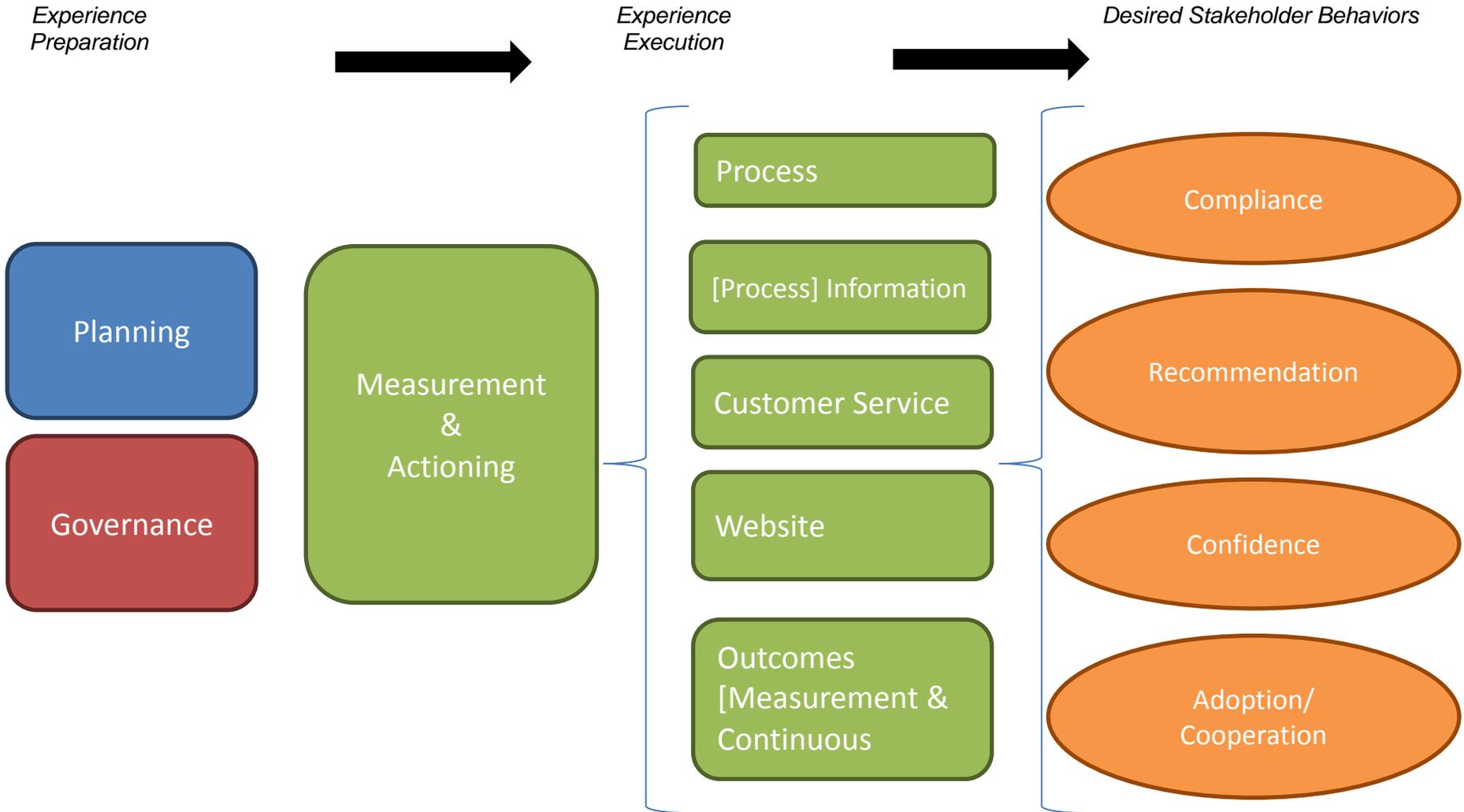
In FY11, the ASR Team evaluated CFPB's performance in the area of Consumer Response (CR). Specifically, we examined the extent to which the Bureau had: (1) complied with relevant laws and regulations; (2) achieved organizational goals and objectives; and (3) aligned with industry best practices. Our analysis in FY11 was guided by an overall framework informed by both general customer experience management best practices and a behavioral model originally developed by the American Customer Satisfaction Index (ACSI) to provide insight into consumer satisfaction with local and federal government services (i.e., the American Consumer Satisfaction Index™ Government Model)<sup>10</sup>. The resulting framework, diagrammed in the figure on the next page, contains three main components—*experience preparation*, *experience execution*, and *desired stakeholder behaviors*.

- Experience Preparation includes activities such as: (1) defining and segmenting key operational stakeholders; (2) gathering insight from stakeholders on their needs and expectations relative to Consumer Response activity; (3) crafting a strategy to address stakeholder needs and deliver the desired experience; and (4) defining clear roles, responsibility and accountability for ideal experience delivery.
- Experience Execution focuses on embedding key elements of the ideal experience strategy and regular stakeholder feedback into daily operating processes, policies, and systems. Execution begins with implementing key business processes that reflect stakeholder needs (e.g., intake, tracking/resolution and analysis/reporting processes). Beyond this, successful experience execution is dependent on multiple related factors, including: (1) providing clarity to stakeholders around key business processes; (2) administering effective communication channels for stakeholders; and (3) instituting process and outcome measurement capabilities and using insight from measurement for the purposes of continuous improvement.
- Desired Stakeholder Behaviors are unique to each entity, but for CFPB were expected to include: (1) stakeholder agreement that the bureau is delivering on its legislative mandate; (2) stakeholder willingness to recommend existing CFPB Consumer Response processes to others; (3) stakeholder confidence in CFPB Consumer Response processes and personnel; and (4) stakeholder cooperation, co-development and/or compliance with CFPB policies, processes and guidance.

---

<sup>10</sup> The American Customer Satisfaction Index, (ACSI) is a private company originally founded in 1994 through the partnership of the University of Michigan/Ross School of Business, the American Society for Quality, and Claes Fornell International. The ACSI interviews about 80,000 Americans annually and asks about their satisfaction with the goods and services they have consumed. Respondents address a wide range of business-to-consumer products and services, including durable goods, services, non-durable goods, local government services, federal government services, etc. Results from data collection and analyses are released to the public throughout each calendar year and utilized to inform and test behavioral models that connect product/service provider actions with desired customer outcomes (e.g., satisfaction, willingness to purchase and/or recommend). The American Consumer Satisfaction Index™ Government Model is one of these models.

### Consumer Response Evaluation Framework



Based on the analysis conducted in FY11, we made 43 recommendations and suggestions related to performance elements in the area of Consumer Response.<sup>11</sup> Included on this list was a broad spectrum of items, ranging from specific corrective actions, to long-term strategic initiatives. Of these 43 performance elements, 4 were reassigned to the Information Technology review area for FY12 evaluation.

The purpose of this FY12 performance audit is to: (1) evaluate the extent to which CFPB has addressed each of the recommendations and suggestions offered in FY11; and (2) provide new or updated recommendations for FY12, to address any residual performance gaps. These “residual recommendations” have been grouped based on severity into one of the categories defined in Section 1.3.3.

## 6.2 Findings and Recommendations

In general, we found that the Bureau has made significant progress towards addressing the 39 CR-related recommendations and suggestions identified in the FY11 Audit Report. Since FY11, multiple CR sections have made advancements in fundamental process infrastructure that will allow the Bureau to achieve its mission over time. Operations appear closest to steady-state within Intake, particularly in those areas dependent upon the operations of the Bureau’s contact center. Investigations is building its capabilities, and Data has implemented a dashboard for performance measurement. Section charter work is underway to continue to clarify the division of labor within and across different operational areas.

Based on the Bureau’s demonstrated performance, we assigned a status of “Closed” to 38 of the 39 FY11 recommendations and suggestions (97%), indicating that no formal corrective action is needed. Included among these closed items are 4 performance improvement opportunities, where suggestions are provided but no corrective action is required. The remaining item is classified as a risk of deficiency or noncompliance, which requires corrective action.

### 6.2.1 Summary of Demonstrated Performance

Table 7 presents the following information for each of the significant performance issues and performance improvement opportunities contained in the FY11 report:

- **Recommendation Statement.** This column states the recommendation or suggestion that was provided in the FY11 Audit Report and provides a unique ID code for each.
- **Summary of CFPB Corrective Actions.** This column reports information about: (1) the actions that CFPB has taken to address the recommendation; (2) plans that CFPB has put in place to address the recommendation; and (3) the status of CFPB’s efforts to address the recommendation.
- **FY12 Status.** This column reports the ASR Team’s assessment of whether or not additional action is required to address the recommendation. A status of “no further action required” indicates that no further corrective action or monitoring is needed with

---

<sup>11</sup> At the start of our FY12 audit process, 4 of the 43 CR-related recommendations from FY11 were moved into the Information Technology review area, because of their focus on CFPB website usability and functionality. As a result, this section focuses on 39 of the 43 recommendations and suggestions from FY11.

respect to the recommendation—either because it has been achieved, or because the Bureau’s ongoing operational and management activities provide adequate control over the recommended action.

## 6.2.2 Significant Performance Issues

In this section, we identify residual recommendations related to performance issues from FY11 that require additional action. For each, we document: (1) the categorization of the residual performance issue based on its FY12 severity; (2) the criteria, condition, cause, and effect associated with the performance issue; and (3) our recommendations for addressing the performance issue.

**2012.CR.1 Respond to written inquiry to contact center SLAs (Risk of Deficiency or Noncompliance).** Consumer Response's outsourced contact center provider (Vangent) receives and processes all consumer written inquiries and faxes, along with most inquiries or complaints registered via phone or the web. For online or phone inquiries, CR has documented clear service level agreements (SLAs) by which Vangent is or will soon be held accountable for performance across most of its intake operations. However, no formal SLA exists for response to written inquiries. Without a comprehensive set of SLAs that tie to the entirety of contact center activity, the Bureau can ultimately hamper its ability to comply with Section 1034(a) of the Dodd-Frank Act, which requires the CFPB to establish “reasonable procedures to provide a timely response to consumers.” Therefore, we recommend that Consumer Response add response to written inquiry expectations to formal contact center SLAs.

**Agency Response.** The Bureau concurs with this recommendation and notes that Consumer Response, in coordination with its strategic partners, is currently in the process of evaluating and enhancing all service level agreements with the outsourced contact center provider to include written inquiries from consumers. This task is part of a larger effort to assess and improve CFPB’s ability to oversee and refine the quality of the entire outsourced contact center.

## 6.2.3 Performance Improvement Opportunities

Below, we present information on aspects of performance related to FY11 performance issues that we believe could be improved, but do not require corrective action. For each of these performance improvement opportunities, we offer suggestions for future action, and we summarize the criteria on which these suggestions are based.

**2012.CR.2 Implement a contact center “customer satisfaction” survey.** Organizations demonstrating best-practice customer experience management behaviors systematically collect and leverage end-user satisfaction/performance assessment feedback with regard to major business operations. Consumer Response’s contact center—either via phone, web chat, mail, or fax—represents one of the CFPB’s major intake mechanisms for consumer complaints. However, the Bureau does not currently collect systematic feedback from contact center users, although they have stated the intention to begin such an activity in the future. Operating a set of intake channels without gathering specific, actionable feedback from its users on their experiences with those channels significantly limits the Bureau's ability to understand and optimize its overall operational performance—regardless of whether CR decides to pursue a more comprehensive feedback platform over time. For these reasons, we recommend that Consumer Response implement a contact center customer satisfaction survey. To the extent that consumers are also not yet systemically intercepted for

feedback on their experiences using CFPB's online "Submit a Complaint" functionality, closing this gap (perhaps by leveraging similar survey questions across both the contact center and web form channels) would allow the Bureau to have a nearly comprehensive understanding of how well it is facilitating the centralized collection of consumer complaints, as referenced in Section 1013(b)(3)(A) of the Dodd-Frank Act.

**2012.CR.3 Implementation of standard on-boarding program and consistent standards for role-specific training across CR Sections.** An organization's ability to consistently address key American Consumer Satisfaction Index™ Government Model satisfaction drivers (e.g., courtesy and professionalism of service, clarity and accessibility of information, or ease and timeliness of service processes) depends in part upon how consistently staff acts on behalf of the organization, in a manner consistent with its mandate and strategy. Starting with Intake, different sections within CR are at different stages of developing and applying training programs specific to that section's own operations and desired stakeholder experience, but there is no standard framework for training programs across sections, nor is there a set of uniform content that speaks to CFPB as a whole. Given the intensity of its anticipated hiring activity through FY13, having new staff in new roles without common training and on-boarding could adversely impact CR's future ability to execute its operations effectively and efficiently. For these reasons, we recommend that CR develop and implement a standard on-boarding program for CR staff and consistent standards around role-specific training across Sections. This training should explain how individual role assignments contribute to overall CFPB mandates and the delivery of its ideal-state consumer/stakeholder experience. It should also include information on the division of labor within and across various major roles and sections. Several of CR's current standup activities (e.g., PPP QA program charter development, CR section charters and related survey work, etc.) can inform eventual training content.

**2012.CR.4 Implementation of policy for periodic feedback analysis and communication of key themes and implications across CR.** To date, Consumer Response has established the basic infrastructure and guidelines for classifying and distributing a broad set of individual contacts classified as "feedback," whether received via phone, mail, fax or other online channels (e.g., CFPB's "Tell Your Story" functionality). Today, the sample size of this unsolicited feedback is not high enough to do periodic proactive analysis and reporting. When Consumer Response achieves a critical mass of feedback sufficient to begin regular analyses, not proactively mining it could cause the Bureau to miss valuable insight with potential implications for policy and/or operations. As mentioned earlier, leveraging feedback from stakeholders (including consumers) wherever it may be captured is a key tenet of best-practice customer experience management. Therefore, we recommend that CR establish and apply a policy for periodic proactive analysis of feedback, and communication of key themes and implications to CR and overall Bureau leadership.

**2012.CR.5 Establishment of an overall "stakeholder feedback platform" strategy.** CFPB has the chance, early in its existence, to formally think through and document its broader strategy for collecting, analyzing and using stakeholder feedback – and to periodically re-evaluate the feedback collection activities it employs. Taking advantage of this approach can help the Bureau "work smart" – focusing its data collection and analysis resources on those actions that will bring the greatest benefits to Consumer Response in particular and the CFPB overall. We recommend that CR prepare a plan to define and document its comprehensive "stakeholder feedback platform." Ideally, this plan would identify:

- Key stakeholder audiences

- Key feedback objectives associated with each stakeholder. This would include the kind of information the Bureau wants to systematically gather from a given stakeholder audience, and why (e.g., to test CFPB's perceived effectiveness in executing its mandate, or to improve its operational efficiency)
- The feedback collection mechanisms that the Bureau either already uses or intends to use to gather the desired information from each stakeholder audience (e.g., post-complaint/investigation survey, advisory board, other meetings/discussion forums, other commissioned research, etc.)
- How feedback gathered from each mechanism is (or will) be embedded into operational improvement across the Bureau in general, or within Consumer Response in particular
- How the Bureau intends to periodically evaluate the utility of different feedback channels to determine whether future platform revisions should be made, in the spirit of continuous improvement

**Table 7: Actions Taken by CFPB to Address Recommendations from the FY11 Audit Report**

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
| Set and enforce target(s) for Contact Center Service Level Agreement performance (2011.CR.8.1) | <ul style="list-style-type: none"> <li>• Performance targets for Contact Center Service Level Agreement (SLA) went into effect November 1, 2011</li> <li>• Per CFPB, historical performance vs. SLA has been high, with the possible exception of telephone call efficiency. To date, there is a single "one size fits all" standard for maximum call length (15 minutes) - irrespective of the nature of product-specific inquiries or complaints</li> <li>• CR leadership (e.g., Section Chief – CR intake) is briefed regularly on key SLA metrics</li> <li>• Weekly meetings held with contact center contractor (Vangent) to review performance versus SLAs, upcoming projects, issue mitigation, etc.</li> </ul>  | Closed                                 |
| Set and enforce target(s) for Response to phone inquiry – Tier I or II (2011.CR.8.2)           | <ul style="list-style-type: none"> <li>• CR contact center SLAs are tied to phone inquiries irrespective of tier</li> <li>• CR holds Vangent responsible in totality for the immediate response to phone inquiry target regardless of the title of the role responsible for this response (for Tier I: CSRs respond, for Tier II: contact center supervisors respond)</li> </ul>  | Closed                                 |
| Set and enforce target(s) for Response to phone inquiry – Tier III (2011.CR.8.3)               | <ul style="list-style-type: none"> <li>• Tier III line is staffed by internal CR intake specialists - they use the same case management system and status items as contact center CSRs use</li> <li>• Tier III training was rolled out to staff in November 2011</li> <li>• Whenever possible, intake specialists answer Tier III inquiries immediately; otherwise, the inquiry is marked as unanswered in RightNow. CE&amp;E then reviews inquiries marked as unanswered and posts responses to most common of the unanswered items on CFPB's website</li> <li>• Scripting in place directs intake specialists to inform a caller with an "unanswered" inquiry to check back on CFPB's website for an eventual response. In this way CR is operating under the expectation that all Tier III inquiries should be addressed upon initial inquiry (even if "addressed" means informing the caller that no official response is available at this time)</li> <li>• CR has interest in triggering a more automated alert to consumers if/when an answer is posted on the CFPB website. To date, there is no formal analysis of whether individuals making phone inquiries ultimately classified as Tier III are satisfied with the current disposition approach or the quality/completeness of responses if/when they are available on the CFPB website</li> </ul> | Closed                                 |
| Set and enforce target(s) for Acknowledgement of written inquiry (2011.CR.8.4)                 | <ul style="list-style-type: none"> <li>• Consumer Response's outsourced contact center provider receives and processes all consumer written inquires and faxes. Inputting a case into RightNow generates an automatic acknowledgement for inquiries regardless of channel (phone, fax, mail)</li> </ul>   | Closed                                 |

| FY11 Recommendation Statement (ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations   |
|---|---|--|
|   | <ul style="list-style-type: none"> <li>• Per "40.4 - Vangent Service Level Agreements":                             <ul style="list-style-type: none"> <li>○ Mail Processing (Time to Input Case) 98% within 1 day (by end of next business day) will become a monthly tracked metric beginning 9/1/12, transitioning to an incented metric by 10/1/12.</li> <li>○ Fax (Time to Input Case) 98% within 1 day (by end of next business day) will become a monthly tracked metric beginning 9/1/12, transitioning to an incented metric by 10/1/12.</li> </ul> </li> </ul>  |  |
| Set and enforce target(s) for Response to written inquiry (2011.CR.8.5)   | <ul style="list-style-type: none"> <li>• Consumer Response's outsourced contact center provider receives and processes all consumer written inquires and faxes; SLAs that tie to the acknowledgement of a written inquiry will be in place as incented metrics by 10/1/12.</li> <li>• However, no formal SLA today exists with the contact center for response to written inquiry.</li> <li>• Evidence of corrective action plans exists around reducing open inquiries and improving online Knowledge Base content to address frequently-posed inquiries ("Inquiry Clean-Up Task Force"/"Inquiry Strategy").</li> </ul>  | Additional Action Required<br>2012.CR.1 (Risk of Deficiency or Noncompliance): Add response to written inquiry to contact center SLAs. |
| Set and enforce targets for response from bank/regulator to consumer – initial complaint (2011.CR.8.6)                          | <ul style="list-style-type: none"> <li>• For Consumer Response's July 21, 2011 launch, the bank's "timely response" requirement was set to 10 business days.</li> <li>• On December 2, 2011, after receiving industry and bank feedback, this requirement was changed to 15 calendar days.</li> <li>• The bank's set target is tracked via the RightNow system. Compliance with this target is shared with Supervision/Enforcement and with the public via the Consumer Complaint Database.</li> <li>• After 30 days with no response or 60 days for cases coded by a bank as "in process" but not yet resolved, complaints are automatically categorized in the CFPB company portal as "no response," triggering an investigation by CR staff.</li> </ul>  | Closed   |
| Set and enforce targets for elapsed time – 1 <sup>st</sup> , 2 <sup>nd</sup> , 3 <sup>rd</sup> tier investigation (2011.CR.8.7) | <ul style="list-style-type: none"> <li>• Investigators are currently held responsible for two primary metrics – number of first-level (1<sup>st</sup> tier) reviews completed (volume) and rework percentage (quality). Note that if an investigation does not require peer (2<sup>nd</sup> tier) or supervisory (3<sup>rd</sup> tier) review, it is deemed complete. "Rework" occurs when an investigation is deemed to require additional review.</li> <li>• Investigators can see how they perform against these metrics via on-demand reporting; managers see summary view reporting to help isolate performance trends. Along with reporting, consistent methodologies were set around how to measure these key metrics (e.g., when it is appropriate for an investigator to receive "credit" for when a 1<sup>st</sup> tier investigation is complete).</li> <li>• Today 100% supervisory reviews occur on all investigations before they are deemed complete (i.e., in effect all</li> </ul> | Closed   |

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
|  | <p>investigations today are 3<sup>rd</sup> tier in nature), but pilot work is underway to allow for more streamlined testing, which may help reduce time to closure for investigations.</p> <ul style="list-style-type: none"> <li>As part of CR's "Operational Metrics Phase I" project, total Investigations cycle time (i.e., from start of investigation to ultimate close) will become a tracked metric.</li> <li>Investigations would like to further track sub-cycle times associated with 1<sup>st</sup>, 2<sup>nd</sup> and 3<sup>rd</sup> tier/supervisory reviews, but this is not in scope for Phase I and future development will be subject to resource availability.</li> </ul>   |  |
| Set and enforce targets for response from bank/regulator – inquiries tied to 1st, 2nd, 3rd tier investigations (2011.CR.8.8)     | <ul style="list-style-type: none"> <li>Currently enforced SLA for response to an investigator request for information is 10 calendar days. Current model is to conduct all activity (e.g., requests for information, responses) within the boundaries of the portal.</li> <li>Instances of non-compliance trigger interaction between Stakeholder Management and the company to determine whether non-compliance is a result of technical issues, training issues or purposeful neglect. No delays to date have been determined to be associated with "purposeful neglect."</li> </ul>   | Closed                                 |
| Set and enforce target(s) for Investigation analysis and tracking (2011.CR.8.9)  | <ul style="list-style-type: none"> <li>In addition to periodic management reports, key metrics around investigation types and volumes are documented in CR's case summary dashboard. This includes aging by queue and status information.</li> <li>Investigations also examines sample cases; ideally, July cases are sampled in early August and results shared in September.</li> <li>More formal report for capturing key analysis themes and takeaways is just being put into place as of August 2012.</li> <li>The "Escalated Case Management" function was started in June 2012 to deal with investigations triggered because consumer says s/he not satisfied (e.g., complaint filed with ombudsman). This group is beginning to informally track trends in complaints and share with CR leadership. A more formal process of periodic analysis and actioning is not yet established, although it is in development.</li> </ul> | Closed                                 |
| Set and enforce targets for Consumer dispute resolution rate (2011.CR.8.10)  | <ul style="list-style-type: none"> <li>Definition: % of "resolved" complaints that consumers subsequently dispute. CR does not use consumer dispute rate as a performance metric, since rates are ultimately subjective and the result of individual consumer perceptions.</li> <li>Consumer Response has produced reports analyzing dispute rates. These reports are used as an input into more robust Investigations volume forecasting.</li> <li>Per both the Data Team and Investigations, this work was de-prioritized after May 2012 in favor of other activities and is not being used regularly by Investigations.</li> <li>However, incorporating investigations rework rate into CR's Case Summary Dashboard is a future initiative.</li> </ul>  | Closed                                 |
| Keep foundational stakeholder research and feedback collected during initial CR and CR credit card functionality standup in mind | <ul style="list-style-type: none"> <li>One of Stakeholder Management's major activities is conducting conversations with companies to gather feedback on what is and is not working within existing complaint resolution processes and systems.</li> <li>Feedback themes then trigger enhancements to the company portal-enabled system as it was originally built</li> </ul>  | Closed                                 |

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
| when rolling out remaining product functionality (2011.CR.9.1)   | <p>based on foundational research.</p> <ul style="list-style-type: none"> <li>Beyond feedback shared during live meetings, companies have had other channels in which to provide comments. Prior to this year, CR received feedback via a dedicated e-mail address, which would then be mined for improvement opportunities. In 2012, CR built an online ticketing system to facilitate feedback collection.</li> </ul>   |  |
| CR may want to invest in supplemental research if/when CR explores additional functionality tied to niche consumer segments (e.g., elderly) (2011.CR.9.2)  | <ul style="list-style-type: none"> <li>Per CFPB, "Consumer Response works with the Office of Servicemember Affairs and Office of Older Americans to assist in the execution of statutory mandates related to their niche consumer segments."</li> <li>As CR prepares for new a product launch, it works with the Offices of Research, Markets &amp; Regulations (RMR), Supervision/Enforcement and Consumer Education &amp; Engagement to convene a task force to give a picture of the full market for the new product.</li> <li>Together, the task force identifies key information gaps that may trigger additional consumer or other stakeholder research/interaction. Another common activity across launches is testing associated with process forms and/or relevant website functionality.</li> </ul>   | Closed                                 |
| To maximize transparency/clarity, consider producing mapping document with stakeholder name/type, key suggestion(s), existing related functionality and planned functionality with expected due dates. (2011.CR.9.3) | <ul style="list-style-type: none"> <li>CR's forum for communicating how stakeholder feedback influences operations is via regular training events delivered via Live Meeting format.</li> <li>The typical format for said training is to point out areas where feedback was provided, how CR been able to improve system, process or policies related to the company portal and finally to point out areas where CR has not yet been able to make changes.</li> </ul>   | Closed                                 |
| CR should create single master project plan/calendar if it does not exist today (2011.CR.9.4)  | <ul style="list-style-type: none"> <li>A project plan/schedule and related weekly review and management process exists for all CR projects requiring IT development assistance.</li> <li>Weekly management review meetings complement the more formal governance process associated with predominantly IT-related system development work.</li> <li>Per CFPB, outside IT development projects, project management practices and styles vary by section/individual.</li> <li>While CR has no master project plan or calendar that allows for consistent leadership visibility across its full portfolio of major section initiatives, CR's weekly management review meetings and project governance meetings collectively allow a forum for review and discussion of section performance (e.g., operational metrics) and key initiative status.</li> </ul> | Closed                                 |

| FY11 Recommendation Statement (ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations                |
|---|---|---|
| CR should clearly isolate critical dependencies associated with the calendar/plan (2011.CR.9.5)   | <p>See row above.</p> <ul style="list-style-type: none"> <li>CR conducts risks assessments for all projects that fall within CR's Governance Committee scope.</li> <li>The same process/approach is not consistently applied across all CR projects, although it does cover most major initiatives for CR.</li> </ul>   | Closed  |
| CR should leverage any upcoming strategic planning/ budgeting activity to bolster plan documentation (2011.CR.9.6)  | <ul style="list-style-type: none"> <li>Consumer Response reports performance metrics to the Director's Office (Office of Strategy) as part of the CFPB strategic initiative and to the CFO office.</li> <li>Consumer Response has yet to formalize strategic plans that link to Consumer Response projects.</li> <li>Operational metrics for Consumer Response are included in the [draft] CFPB Strategic Plan and tie to Bureau Outcomes and Goals.</li> <li>The Bureau's most recent performance review occurred in August 2012 and contains performance and corrective action information associated with Consumer Response.</li> </ul>  | Closed  |
| CR should include process measures and targets associated with individual roles in position descriptions / performance management expectations; tie to rewards/ recognition. (2011.CR.10.1) | <ul style="list-style-type: none"> <li>The process measures and targets associated with Consumer Response employee performance are evidenced in the Consumer Response Performance Level Standards Manual, revised periodically.</li> <li>More detailed targets and measures relative to individual roles are excluded from the position descriptions, which are subject to modification, but are part of individual performance plans.</li> <li>The latest copy of the performance manual is stored on the Bureau's shared drive; each supervisor provides individual with a copy as s/he drafts his/her performance plan.</li> <li>CR complies with the Bureau's overall policy on performance to address issues if/when individual staff members are deemed to warrant an "unacceptable" rating.</li> </ul> | Closed  |
| Consider formal division of labor/RACI document as systems normalize - as single go-to artifact of roles, responsibilities within and across entities for major functions (2011.CR.10.2)    | <ul style="list-style-type: none"> <li>Consumer Response is examining the division of labor within CR relative to the broader Bureau.</li> <li>To inform this analysis, CR collected data from the Assistant Director and Section Chiefs, which is being used as the basis for creating roles and responsibilities charters for each Consumer Response Section.</li> <li>Completed charters will go out on the Bureau's wiki site.</li> <li>Planned milestones and anticipated dates are: completion of Section Chief Interviews by September 14, 2012; completion of Section charters by October 1, 2012.</li> </ul>   | Closed  |
| If CR chooses to create a formal division of labor/RACI document, it should create this collaboratively with stakeholders for maximum impact (2011.CR.10.3)                                 | <ul style="list-style-type: none"> <li>Per CR leadership, "Consumer Response will coordinate with stakeholders to define roles and responsibilities." Planned milestones and anticipated dates are:                             <ul style="list-style-type: none"> <li>Coordinate with stakeholders - October 1 through November 1; today, "stakeholders" is assumed to encompass other offices within the Bureau.</li> <li>Complete documentation of roles and responsibilities - November 15.</li> </ul> </li> </ul>  | Closed  |
| CR should explore linking both target and rationale within staff training for educational   | <ul style="list-style-type: none"> <li>Consumer Response's Investigations group develops materials that emphasize CFPB's strategic goals and CR's objectives. These materials are created by Investigations, for Investigations. Supplied materials are listed</li> </ul>   | Additional Action Suggested<br>2012.CR.3 (Performance |

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations  |
|--|--|---|
| <p>purposes (2011.10.4)</p>  | <p>as "pre-decisional."</p> <ul style="list-style-type: none"> <li>CR Intake also trains its own intake specialists and has applied this to its first cohort as of August 30, 2012. Program includes: orientation on role expectations/rationale, job shadowing, working in testing environment, team lead "mentor" assignment during training period. Intake also helps develop and implement training for Vangent contact center staff.</li> <li>However, there is no common on boarding program or consistent training framework across Consumer Response.</li> <li>Consumer Response is in the process of hiring a training director and a strategic planning analyst, who will: (1) ensure that all staff training continues to address Consumer Response's strategic goals and targets, and the rationale for them; and (2) educate new staff in the nexus of their roles and responsibilities and CFPB's mission, goals and objectives.</li> </ul>  | <p>Improvement Opportunity): CFPB should develop and implement standard onboarding for CR staff and consistent standards around role training (and linkage to key operational goals and targets) across Sections.</p> |
| <p>CR should ensure that relevant metric definitions are easily accessible within any future dashboard reporting CR adopts (2011.CR.10.5)</p>  | <ul style="list-style-type: none"> <li>Consumer Response has developed a foundational dashboard report.</li> <li>On May 15, 2012 Consumer Response incorporated definitions for relevant metrics into the dashboard version distributed weekly.</li> <li>As additional operational metrics for cycle time and rework are added, the related definitions will either be integrated into the dashboard itself or into a supporting document.</li> </ul>  | <p>Closed</p>   |
| <p>CFPB should consider enhancing future intake specialist, investigator and QA/QC staff capabilities via certification programs. (2011.CR.10.6 (CR43.6), Performance Improvement Opportunity)</p> | <ul style="list-style-type: none"> <li>Per CR leadership: "The Consumer Response Section Chiefs discussed the recommendation regarding staff certifications and decided not to take action at this time, but would consider a future analysis to determine the need and feasibility of establishing certification requirements for Consumer Response positions."</li> </ul>  | <p>Closed</p>   |
| <p>CR should monitor user comments for navigational ease past initial intake page - consider adding to website functionality (2011.CR.11.1)</p>  | <ul style="list-style-type: none"> <li>CR's Data Management and Analysis team shares information through multiple channels. Within CR, all existing feedback channels (phone, mail, web, etc.) are referred to as "Tell Your Story." This is a broader definition than the actual "Tell Your Story" functionality within CFPB's website.</li> <li>In early August 2012, Consumer Response began routing to the Technology &amp; Innovation team feedback about the website, such as feedback about the navigational ease past the initial intake page.</li> <li>By the end of August 2012, all feedback tagged for the Technology and Innovation team will be routed automatically, consistent with routing of other feedback.</li> <li>Today the total volume of feedback is not high enough to do regular feedback analysis, but the system contains enablers to do so. CR does receive ad-hoc requests for information from the feedback today, primarily from other areas within CFPB, and responds as requested.</li> </ul> | <p>Closed</p>   |

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations   |
|--|--|--|
| <p>CR should implement contact center customer satisfaction survey as soon as possible (2011.CR.11.2)</p>  | <ul style="list-style-type: none"> <li>Consumer Response has stated that it is currently developing requirements for a future procurement, to obtain consulting support in the development and deployment of a multi-channel consumer satisfaction survey. However, as of October 5, 2012, CR was unable to provide the audit team with any documentary evidence of this activity.</li> </ul>  | <p>Additional Action Suggested<br/>2012.CR.2 (Performance Improvement Opportunity): CR should implement contact center customer satisfaction survey as soon as possible.</p> |
| <p>CR should consider employing "universal contact code" to enable easy tracking of contacts as information flows back and forth across regulators. (2011.CR.11.3)</p>               | <ul style="list-style-type: none"> <li>Every complaint, inquiry or feedback created on the Consumer Response case management system (RightNow) is assigned a unique identifying number (case number).</li> <li>Unique case numbers are then associated with the primary contact on the case (person who contacted CFPB) via a main contact record. This record lists the consumer, his or her contact information and all cases where they have been identified as the primary contact.</li> <li>RightNow data is searchable by contact last name and case number, among other fields.</li> </ul>  | <p>Closed</p>  |
| <p>CR should continue with relevant QC and data hires to resource measurement, inspection, reporting and related analysis (2011.CR.11.4)</p>   | <ul style="list-style-type: none"> <li>Consumer Response now has three data analysis staff, including a data manager hired in June 2012.</li> <li>In August 2012, the Data Manager posted and selected three additional data staff (research, quality, and reporting); all three accepted, and all 3 will have started by 9/25/12.</li> <li>Vangent staff members support contact center analytics (see SLAs and information in 40.1 and 44.5).</li> <li>CR obtained additional data support from PriceWaterhouseCoopers and Vangent. In addition to actual application development work, PwC has provided a Lean Six Sigma (L6S) black belt resource that is partnering with CR on any project tied to operational metrics and reporting appropriate for the section chief/manager level.</li> <li>Consumer Response is currently reviewing certificates received for the vacancy announcement for Section Chief for Data.</li> </ul> | <p>Closed</p>  |
| <p>CR should continue to mine channel usage information to determine whether it needs to adjust hours of operation/access for non-internet-based channels. (2011.CR.11.5)</p>        | <ul style="list-style-type: none"> <li>Communications volume is tracked and reported via contact center SLA management processes, and communicated internally to CR and CFPB leadership.</li> <li>Tracking of Tier III inquiry volumes has triggered re-evaluation of staffing levels.</li> </ul>  | <p>Closed</p>  |
| <p>CR should continue building notifications capability/consumer portal access to allow for more robust status/tracking capability (i.e., notify consumer as investigation moves</p> | <ul style="list-style-type: none"> <li>Consumers can log into CFPB's Consumer Portal and check the status of their complaints once they are filed. The same information is available to the consumer via the contact center.</li> <li>Progress through the complaint resolution process triggers automatic mail or email messages to the consumer:                             <ul style="list-style-type: none"> <li>When complaint is first filed.</li> </ul> </li> </ul>  | <p>Closed</p>  |

| FY11 Recommendation Statement (ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
| through tiers, as relevant). (2011.CR.11.6)   | <ul style="list-style-type: none"> <li>○ When initial response is received from the company.</li> <li>○ When complaint is escalated to an investigation (if applicable).</li> <li>○ When CFPB investigations completes its work.</li> </ul>  |  |
| CR should accelerate standup of call center QC activity and related coaching/training for individual CSRs to improve consistency of consumer contact experience (2011.CR.11.7)              | <ul style="list-style-type: none"> <li>● All new contact center CSR hires go through a training program, including a review of all CR-covered products.</li> <li>● After completion of training, CSRs move on to a “nesting program, “ using QA monitors and supervisors to provide support throughout the “nesting” period.</li> <li>● After “nesting,” CSR’s are certified but still have an assigned coach.                             <ul style="list-style-type: none"> <li>○ A deputy project manager for Vangent oversees the contact centers and maintains an on-site presence at CFPB offices for connectivity.</li> <li>○ No terminations have had to take place to date due to a CSR not satisfactorily completing on boarding.</li> </ul> </li> <li>● When new products come out – RMR and CR representatives visit contact center staff to provide training on the new products</li> </ul> | Closed                                 |
| CR should explore potential to accelerate adoption of SLA before November 1, 2011 (2011.CR.11.8)  | <ul style="list-style-type: none"> <li>● Performance targets for Contact Center Service Level Agreements went into effect November 1, 2011.</li> </ul>   | Closed                                 |
| CR should monitor user comments for [website] navigational ease/utility; can leverage low cost existing tools to get general experience feedback (e.g., 4Q) (2011.CR.11.9)                  | This performance element is evaluated in the IT section.   |  |
| CR should consider moving "Building the CFPB" placement as functionality expands, to make room for clear calls-to-action associated with critical complaint intake activity (2011.CR.11.10) | This performance element is evaluated in the IT section.   |  |
| CR should consider reducing height of the homepage to minimize vertical scrolling   | This performance element is evaluated in the IT section.   |  |

| FY11 Recommendation Statement (ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
| (2011.CR.11.11)   |  |  |
| CR should consider modifying text included in images on the CFPB homepage; images cannot be read by search engines (Google, Yahoo, Bing) therefore, rank lower in search results. (2011.CR.11.12) | This performance element is evaluated in the IT section.   |  |
| CR should continue implementation of contact center QA plan (2011.CR.11.13)   | <ul style="list-style-type: none"> <li>Consumer Response and Vangent started to measure CSR performance and overall customer service on November 1, 2011. The measurement Scorecard has since been implemented within Consumer Response's Call Quality Monitor Software known as EyeQ360.</li> <li>CR is currently recruiting for a QA Team Lead as well as QC Monitor to focus on non-phone related functions performed by the contact center including mail, fax, and inbound referral processing.</li> <li>A major driver of QA with regard to the contact center is ensuring that data is inputted correctly so that complaint information can be passed to companies and resolved. To this end, CR is working with Booz Allen to analyze the satisfaction of CR's intake specialists and identify QA and other process improvement actions to implement at the Contact Center.</li> </ul> | Closed                                 |
| CR should get non-contact center operations to same level of metrics visibility as call center: This may include: (1) Creating automated dashboard (2011.CR.11.14-A)                              | <ul style="list-style-type: none"> <li>CR's Data Management and Analysis (DMA) team has developed a management dashboard.</li> <li>In April 2012, DMA began distributing the dashboard weekly to Section Chiefs and managers.</li> <li>Dashboard functionality currently focuses on volume and work-in-process status versus items like cycle time or rework.</li> <li>The current version of this case summary dashboard is distributed weekly to Section Chiefs and managers.</li> <li>Per CR leadership, an expanded dashboard will be released on Oct. 1.</li> <li>Beyond the dashboard, CR management develops and reviews periodic reports.</li> </ul>   | Closed                                 |
| CR should get non-contact center operations to same level of metrics visibility as call center: This may include: (2) Monitoring no less than 3X per month (2011.CR.11.14-B)                      | See 2011.CR.11.14-A (CR46.5A)  | Closed                                 |

| FY11 Recommendation Statement (ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
| <p>CR should get non-contact center operations to same level of metrics visibility as call center: This may include: (3) Ensuring quarterly review/analysis cycle (2011.CR.11.14-C)</p>  | <p>See 2011.CR.11.14-A (CR46.5A)</p>  | <p>Closed</p>                          |
| <p>CR should get non-contact center operations to same level of metrics visibility as call center: This may include: (4) Developing improvement process and plans for metrics that fall short of standards (2011.CR.11.14-D)</p> | <ul style="list-style-type: none"> <li>• CR's current case summary dashboard focuses on overall operational health and bottlenecks (i.e., volume and throughput). This lets CR leadership see a potential emerging trend for further offline analysis and corrective actions.</li> <li>• CR's "Operational Metrics Phase I" project adds baseline metrics for cycle time and rework requirement rate. Cycle time scope for this work is at two levels - how quickly items move through all stages and relevant sub-cycle times for intake, consumer, investigations, etc.</li> <li>• Target is that by September 30, CR will have a beta version of reporting with cycle times and rework requirement rates daily.</li> <li>• Over the two weeks following launch, (leveraging PwC resources, PPT staff, policy analyst help) CR will review data and determine how to fold into a single master snapshot dashboard, thereby enhancing CR's current case summary dashboard.</li> <li>• Today's case summary dashboard informs the agenda of bi-weekly management team meetings - reviews during these meetings are focused in part on highlighting areas where CR may need to establish improvement processes. Any observations prepared in advance of the management meetings are not formally documented.</li> <li>• Performance improvement activity is primarily driven today via in-line QA resources. CR's PPP team is developing it's a charter, which will include responsibility for the standup of an end-to-end QA process to supplement in-line activity. QA outputs in the future may include policy as well as process improvement implications.</li> </ul> | <p>Closed</p>                          |
| <p>Consumer Response should consider employing concept of an "annual CR scorecard" to summarize key metrics and anticipated improvement initiatives for distribution to full stakeholder base - way to</p>                       | <ul style="list-style-type: none"> <li>• CR relies upon its case summary dashboard to communicate key metrics.</li> <li>• On at least a monthly basis, CR prepares information for CFPB's policy committees.                         <ul style="list-style-type: none"> <li>○ Attendees – assistant directors and other key managers throughout the Bureau.</li> <li>○ The same information is also made available on CFPB's wiki site.</li> </ul> </li> <li>• For external stakeholders, CR relies upon three major publications:</li> </ul>   | <p>Closed</p>                          |

| FY11 Recommendation Statement (ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations  |
|---|---|---|
| formalize feedback collection/use (2011.CR.11.15)   | <ul style="list-style-type: none"> <li>○ CFPB's semi-annual reports (first published January 2012 and July 2012) and</li> <li>○ The Consumer Response Annual Report (last published March 2012).</li> </ul>   |   |
| CR should consider developing parallel team to internal CR steering committee via a formal (rotating membership) stakeholder advisory board (2011.CR.11.16)   | <ul style="list-style-type: none"> <li>● Consumer Response's internal steering committee was discontinued in November 2011.</li> <li>● Per CR leadership "the Consumer Response Section Chiefs considered developing an external stakeholder advisory group, and concluded that the benefits of such an advisory group were more than a year away given where Consumer Response is in its development lifecycle."</li> </ul>  | Closed  |
| CR should establish a single master dashboard to cover core operating metrics as described in citation 40.1 to 40.10 (2011.CR.11.17)  | <ul style="list-style-type: none"> <li>● See Consumer Response.46.5A-C</li> </ul>   | Closed  |
| CR should set internal standards for mining feedback [phone/ web/ mail/ email comments], both as a safeguard to ensure incorrectly coded feedback is rerouted if necessary, and to provide fresh data/analysis on process improvement, emerging consumer concerns/needs, etc. (2011.CR.11.18) | <ul style="list-style-type: none"> <li>● CR prepares reports to highlight selected comments received through web/email/phone; these are available for broad review on the Bureau-wide wiki.</li> <li>● These memos contain intentional qualifiers so anybody who may review these in the future (e.g., via FOIA) understands that the Bureau does not believe that a limited "highlights" memo is representative of the totality of feedback.</li> <li>● Today the aggregate sample size for unsolicited feedback is not high enough to do formal analysis, but the system contains enablers to do so.</li> </ul> | <p>Additional Action Suggested</p> <p>2012.CR.4 (Performance Improvement Opportunity): Implement policy for periodic proactive feedback analysis and communication of key themes and implications across CR.</p> <p>2012.CR.5 (Performance Improvement Opportunity) Establish an overall "stakeholder feedback platform" strategy (i.e., plans to collect, analyze and use stakeholder feedback, and to periodically re-evaluate feedback collection activities).</p> |

## Section 7: Human Capital and Organizational Development

### 7.1 Scope of Audit

In FY11, the ASR Team evaluated CFPB’s performance in the area of Human Capital and Organizational Development. Specifically, we examined the extent to which the Bureau had: (1) complied with relevant laws and regulations; (2) achieved organizational goals and objectives; and (3) aligned with industry best practices. Our analysis in FY11 was guided by the Human Capital Assessment and Accountability Framework (HCAAF), established by the Office of Personnel Management (OPM). Specifically, the HCAAF defines five human capital systems—three of which were used to evaluate the Bureau’s performance: Leadership and Knowledge Management, Results-Oriented Performance Culture, and Talent Management.

Based on the analysis conducted in FY11, we offered 38 recommendations and suggestions related to performance elements in the area of Human Capital and Organizational Development. Included on this list was a broad spectrum of items, ranging from specific corrective actions, to long-term strategic initiatives. The purpose of this FY12 performance audit is to: (1) evaluate the extent to which CFPB has addressed each of the recommendations and suggestions offered in FY11; and (2) provide new or updated recommendations for FY12, to address any residual performance gaps. These “residual recommendations” have been grouped based on severity into one of the categories defined in Section 1.3.3.

### 7.2 Findings and Recommendations

Based on the Bureau’s demonstrated performance, we assigned a status of “Closed” to all of the FY11 recommendations and suggestions (100%), indicating that no formal corrective action is needed. Included among these closed items is one performance improvement opportunity, where suggestions are provided but no corrective action is required.

#### 7.2.1 Summary of Demonstrated Performance

Table 8 presents the following information for each of the significant performance issues and performance improvement opportunities contained in the FY11 report:

- **Recommendation Statement.** This column states the recommendation or suggestion that was provided in the FY11 Audit Report and provides a unique ID code for each.
- **Summary of CFPB Corrective Actions.** This column reports information about: (1) the actions that CFPB has taken to address the recommendation; (2) plans that CFPB has put in place to address the recommendation; and (3) the status of CFPB’s efforts to address the recommendation.
- **FY12 Status.** This column reports the ASR Team’s assessment of whether or not additional action is required to address the recommendation. A status of “no further action required” indicates that no further corrective action or monitoring is needed with respect to the recommendation—either because it has been achieved, or because the Bureau’s ongoing operational and management activities provide adequate control over

the recommended action.

## **7.2.2 Performance Improvement Opportunities**

Below, we present information on aspects of performance related to FY11 performance issues that we believe could be improved, but do not require corrective action. For each of these performance improvement opportunities, we offer suggestions for future action, and we summarize the criteria on which these suggestions are based.

**2012.HC.1 Development of a Long Term Recruitment Strategy.** In accordance with HCAAF standards, the Bureau should establish recruitment, retention, and development efforts to bring the competencies of its workforce into alignment with the agency's current and future needs. To date, CFPB's recruitment strategy has focused primarily on achieving short-term objectives, and staffing up to the target state of its organizational structure. The Bureau has started to develop plans in this area, as evidenced by the Human Capital Strategic Plan, which states that "from 2013 to 2015, OHC will continue its transition from start-up phase activities to more robust, longer term human capital programs." While the present activities are appropriately focused on staffing up critical positions and core functions, a longer term recruiting plan is needed to enable the Bureau to meet future staffing demands in a competitive marketplace. In 2011, we identified a Performance Improvement Opportunity (2011.HC.2.3) related to development of a long-term recruitment plan. We view this as a continuing need.

**Table 8: Actions Taken by CFPB to Address Recommendations from the FY11 Audit Report**

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| <p>CFPB should hire personnel to direct and implement the offices and units functions as required by the Dodd-Frank Act. (2011.HC.1.1)</p>   | <ul style="list-style-type: none"> <li>• The most updated organization chart and briefings of the status of workforce planning indicate that all offices identified in the Dodd Frank Act have been established and are functioning.</li> <li>• All CFPB mission critical positions including Associate Director and Administrative Director positions outlined in the legislation are filled with permanent or acting resources. The CFPB Organization Chart lists the position "Administrative Law Judge" as vacant. However, supporting documentation indicates that CFPB has recently received approval from OPM to hire this position.</li> </ul>   | <p>Closed</p>                          |
| <p>CFPB should identify gaps between projected or actual availability of the CFPB's mission-critical competencies and the current and future demands. (2011.HC.2.1)</p>                    | <ul style="list-style-type: none"> <li>• Gap analysis conducted by CFPB revealed the most critical and current occupation demand for talent acquisition, including Examiner positions and Technology and Innovation positions. CFPB continues to recruit and has focused its efforts on filling specialized positions.</li> <li>• Position Descriptions and behavioral indicator worksheets help to define skills and competencies, and identify behavioral indicators to assist in developing competencies per position and pay band.</li> <li>• Additional talent acquisition assets were developed for multiple mission-critical positions including Examiner and Technology &amp; Innovation positions.</li> <li>• Training materials were developed and used to implement an assessment process for candidate selection. Managers and staff received this training to assess and rate candidates for mission critical positions.</li> <li>• CFPB Core Competencies have been identified for employees Bureau-wide. Planned in the CFPB Strategic Plan FY13-FY15 is to continue to refine competencies and to include subject matter experts and a workforce survey to validate the competencies.</li> </ul> | <p>Closed</p>                          |
| <p>CFPB should staff the vacant critical leadership positions (in FY11, 4 of the 6 Associate Directors were on board and 20 of the 36 Assistant Directors were on board) (2011.HC.2.2)</p> | <ul style="list-style-type: none"> <li>• An approach for recruiting key roles was implemented to fill the vacant Associate Director and Assistant Director positions with mission-critical hires.</li> <li>• Workforce planning and organizational design analysis was completed for each office. Structures were developed and reviewed with each office executive to finalize designs and improve hiring efficiency.</li> <li>• Executive Level competencies and roles have been developed and defined. A "Developing Executives" program was established to define executive level competencies.</li> <li>• A rigorous development program was established to promote executives from within CFPB.</li> <li>• Also see demonstrated performance for item 2011.HC.1.1</li> </ul>   | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations  |
|--|---|---|
| CFPB should develop a long-term recruitment plan. (2011.HC.2.3)  | <ul style="list-style-type: none"> <li>In accordance with HCAAF standards, the Bureau should establish recruitment, retention, and development efforts to bring the competencies of its workforce into alignment with the agency's current and future needs. To date, CFPB's recruitment strategy has focused primarily on achieving short-term objectives, and staffing up to the target state of its organizational structure.</li> <li>The Human Capital Strategic Plan states that "from 2013 to 2015, OHC will continue its transition from start-up phase activities to more robust, longer term human capital programs." While the present activities are focused on staffing up critical positions and core functions, it will be necessary as stated to develop a longer term recruiting plan.</li> </ul>  | Additional Action Suggested<br>2012.HC.1 (Performance Improvement Opportunity): CFPB should develop a long-term recruitment plan. |
| CFPB should focus its long-term recruiting efforts on acquiring specialized competencies necessary to round out workforce. (2011.HC.2.4) | <ul style="list-style-type: none"> <li>In accordance with the CFPB Human Capital Strategic Plan FY13-FY15, the Office of Human Capital (OHC) will conduct annual workforce planning processes that are integrated with the annual budget to identify workforce gaps and proactively plan for mission driven hiring needs.</li> <li>OHC also plans to collaborate with business units to identify and prioritize staffing needs and plans, and monitor hiring progress to close gaps.</li> <li>Also see demonstrated performance for item 2011.HC.2.1</li> </ul>   | Closed  |
| CFPB should develop a formal Human Capital Program Plan, which would build on existing projects and systems. (2011.HC.2.5)               | <ul style="list-style-type: none"> <li>In FY12, CFPB developed and approved a CFPB Human Capital Strategic Plan FY2013 - 2015, which addresses recruitment, engagement and total rewards; learning, development and performance management; and human capital infrastructure strategies.</li> <li>OHC has developed a plan to accompany the Strategic Plan that includes a detailed description of activities, metrics, results, time frames and responsible parties.</li> </ul>  | Closed  |
| CFPB should develop an Executive/Management Development Program. (2011.HC.3.1A)  | <ul style="list-style-type: none"> <li>CFPB has started to create a learning and development program, which includes mandatory training programs for executives and managers. A series of classes were identified for managers to be completed annually.</li> <li>Performance management training was developed and held for executives and managers. The sessions describe the performance management process - developing the IDP, mid-year and annual reviews.</li> <li>Guidance was developed to provide CFPB managers with information on managerial duties and responsibilities.</li> <li>OHC began drafting the outline of a more robust executive/management development program to vet through leadership and roll out in FY13. To support the rollout of what is currently being called "The Innovative Federal Leadership Program", OHC has crafted a plan that aligns with the goals and objectives it hopes to accomplish through the program.</li> <li>Also see demonstrated performance for item 2011.HC.3.1B</li> </ul> | Closed  |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| CFPB should ensure availability of trained mentors to support new and prospective leaders and employees in development programs. (2011.HC.3.1B)                 | <ul style="list-style-type: none"> <li>● CFPB put in place a coaching and facilitation program to mentor and assist new executives at CFPB, and to identify and address strengths and areas of opportunity. The coaching sessions are focused on individual needs for the leaders and their staff; and have been built into the CFPB Executive Career Ladder Program.</li> </ul>  | Closed                                 |
| CFPB should define individual performance plans to rate leaders and managers on their implementation of change initiatives as change is ongoing. (2011.HC.3.2A) | <ul style="list-style-type: none"> <li>● OHC policy provides guidance for leaders and managers to implement change. It clarifies the change management roles for leader and manager, as defined in the Executive Performance Competencies: Leading Change. The Performance competency is further defined as, Creativity and Innovation, External Awareness, Flexibility, Resilience, Strategic Thinking, and Vision.</li> </ul>   | Closed                                 |
| CFPB should document the Bureau's strategy and plan for communication of change. (2011.HC.3.2B)   | <ul style="list-style-type: none"> <li>● CFPB has developed regular methods to communicate change using the following methods:                             <ul style="list-style-type: none"> <li>○ An internal newsletter provides information such as reminders about the performance management period, as well as introductions to new people, their focus and business philosophy. Introductions of Director, Associate Directors, Examiners and others provide insight to who's on board at CFPB. The connection also has sections to communicate and update the bureau on recent events, recognize and commend deserving personnel, and connect people and groups to important activities in an organization that is spread nationally.</li> <li>○ Activities the CFPB Culture Team plans to support and nurture through inter-divisional collaboration and training. They are tasked with onboarding activities, monitoring the CFPBedia "Culture Team" wiki site, monitoring the integration of values, facilitating surveys, hosting lunch &amp; learns, supporting infrastructure projects, and organizing Bureau-wide social events.</li> </ul> </li> </ul> | Closed                                 |
| CFPB should participate in an OPM led, Annual Employee Viewpoint Survey (AES) to provide a mechanism for anonymous employee feedback. (2011.HC.3.3A)            | <ul style="list-style-type: none"> <li>● CFPB identified early the need to develop an employee feedback mechanism with anonymous feedback system to gather timely information. A pulse survey was completed early in FY12 and the Annual Employee Survey has been implemented.</li> <li>● A crosswalk of the questionnaires for the Annual Employee Survey and Pulse Survey was completed. The pulse survey results have been cascaded throughout CFPB and the Annual Employee Survey is in review.</li> </ul>  | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|--|---|--|
| <p>CFPB should establish IDPs including teamwork, collaboration and other mechanisms to drive performance for a highly engaged staff. (2011.HC.3.3B)</p>   | <ul style="list-style-type: none"> <li>• CFPB Employee Equal Opportunity Center of Excellence is developing a plan that incorporates both engagement and inclusion.</li> <li>• Core competencies have been developed that includes Leading People (team building) and Collaboration.</li> <li>• Guiding Principles in the CFPB Performance Management includes: Meritocracy; Values-driven – Serve, Lead and Innovate; Feedback and development; and Accountability.</li> <li>• The CFPB Human Capital Strategy FY13-FY15 states goals, tactics and activities for employment engagement, including: (1) accountability for fostering and promoting a diverse, inclusive and engagement workforce in performance evaluations; (2) create an engagement program that aligns and promotes the CFPB's mission, vision, values, and strategy.</li> </ul>  | <p>Closed</p>                          |
| <p>CFPB should develop a Training and Workforce Development Plan that builds competencies important to strategic goals and objectives, and CFPB's performance plan execution. (2011.HC.3.4A)</p> | <ul style="list-style-type: none"> <li>• CFPB instituted the following training programs: (1) New Employee Orientation; (2) Excellence through Communication and Collaboration (ECC); (3) Mandated Training (required training for all government agencies, including topics such as Cyber-Security Awareness, EEO Training, New Employee Ethics Overview, and Prevention of Sexual Harassment); (4) Supervisory Exam System Training for examiners; (5) On the Job Training (OJT) Program for examiners; (6) Fair Lending Course; (7) Real Estate Lending Course; and (8) Capstone Course.</li> <li>• Technical and non-technical training needs, priorities and recommendations have been identified to support strategic imperatives for the implementation of training and learning program.</li> <li>• The CFPB Human Capital Strategic Plan FY13 -FY15 includes Learning, Development, and Performance Management, and describes the steps needed to develop a 21st century learning organization including a learning, development and performance management plan, including goals and activities.</li> </ul> | <p>Closed</p>                          |
| <p>CFPB should tie competency models to individual development plans for mission critical employees (2011.HC.3.4B)</p>   | <ul style="list-style-type: none"> <li>• Core competencies have been developed for executives, supervisory and non-supervisory employees.</li> <li>• OHC policy defines competencies for executives, supervisory and non-supervisory employees, and establishes a framework for rating officials to review individual performance in the areas of work complexity, independence, and impact.</li> <li>• The performance system was developed and implemented into the inCompass performance system. This system is the tool that ties competency models to IDPs as specified in the Performance Management Program Policy.</li> </ul>   | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| CFPB should define the value of sharing knowledge for reuse and collaboration. (2011.HC.3.5A)   | <ul style="list-style-type: none"> <li>• CFPB developed a wiki site (CFPBedia) and is using the site to store and share knowledge, manage data, and facilitate collaboration.</li> <li>• The CFPB Human Capital Strategic Plan FY 13-FY15, has a tactic to incorporate knowledge management processes within learning programs to promote collaboration and improve business results.</li> </ul>  | Closed                                 |
| CFPB should establish mechanisms such as incentives, or a requirement on individual performance plans, to drive use and reuse data sources. (2011.HC.3.5B)            | <ul style="list-style-type: none"> <li>• CFPB has documented processes, policies, training, etc. stored on the CFPBedia wiki site.</li> <li>• Knowledge management will need to be defined for greater understanding of its value if CFPB has a need to drive use and reuse of data. Knowledge management may be owned and managed by another CFPB office in the future if CFPB determines the need to manage organizational knowledge differently.</li> </ul>  | Closed                                 |
| CFPB should establish a communication strategy that shares the vision, mission, and other related documents, such as the Human Capital Strategic plan. (2011.HC.4.1A) | <ul style="list-style-type: none"> <li>• During the onboarding process/program, CFPB begins communicating the vision, mission and other important information. The culture club is chartered to communicate its vision and mission, and provides links to related information and documents on the wiki site (CFPBedia).</li> <li>• A communication plan will be further developed as stated in the CFPB Human Capital Strategic Plan FY13-FY15, a data-driven engagement and communication strategy that supports a workforce with a strong organizational identity that is committed to the mission and values of the CFPB.</li> <li>• A focal point of the OHC and the Human Capital Strategic Plan describes various methods for recruitment, engagement and total rewards.</li> <li>• Refer to Item 2011.HC.3.2B.</li> </ul> | Closed                                 |
| CFPB should survey employees to gather data that indicates they are aware of the strategic plan and goals. (2011.HC.4.1B)   | <ul style="list-style-type: none"> <li>• Refer to comments in Item 2011.HC.3.3A</li> </ul>  | Closed                                 |
| CFPB should establish division goals that tie to organizational goals. (2011.HC.4.2A)   | <ul style="list-style-type: none"> <li>• CFPB developed a Performance Management training session, "Writing SMART Objectives" which presents directions on how objectives should be established based on the strategic plan. The session discusses how to tie objectives to executive plans, supervisor plans and non-supervisor plans.</li> <li>• The CFPB Human Capital Strategic Plan FY13-FY15, the Performance Management initiative will support the Bureau's mission, vision, and strategy.</li> </ul>   | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| CFPB should integrate organizational goals into the Cornerstone performance management system. (2011.HC.4.2B)  | <ul style="list-style-type: none"> <li>CFPB has implemented performance management in the inCompass system (a Cornerstone tool) across CFPB. This is an online tool used for the performance management process of identifying performance objectives, and for midterm and final review processes.</li> <li>In the inCompass system, each employee creates objectives, and aligns these objectives to strategic goals.</li> </ul>  | Closed                                 |
| CFPB should develop and communicate processes for dealing with poor performance. (2011.HC.4.2C)  | <ul style="list-style-type: none"> <li>OHC policy states and communicates the process for dealing with poor performance.</li> <li>OHC policy describes the CFPB's performance improvement plan for unacceptable performance.</li> </ul>  | Closed                                 |
| CFPB should design, communicate and implement a formal award program that aligns with organizational goals and values. (2011.HC.4.3A)                      | <ul style="list-style-type: none"> <li>CFPB has developed a program to incentivize exceptional performance that results in significant achievements. Type of Awards include: Monetary Awards, Time off Awards, and Non-Monetary Awards. The policy details all the Monetary and Non-Monetary Awards, who initiates, approves, and other parameters.</li> <li>CFPB Human Capital Strategic Plan FY13-FY15, states that the CFPB will work with stakeholders to continually refine and enhance the CFPB's total rewards program in order to motivate, sustain, and retain the existing workforce.</li> </ul> | Closed                                 |
| CFPB should establish proposed awards such as merit pay, short-term incentives, recognition programs, and other performance award programs. (2011.HC.4.3B) | <ul style="list-style-type: none"> <li>CFPB has developed workforce flexibility programs and written associated policies. Some of the completed polices include Telework, Alternate Work Schedule, Sick Leave, External Training, etc.</li> <li>There are additional polices in development and in queue regarding award programs.</li> </ul>  | Closed                                 |
| CFPB should establish clear pay distinctions for performance in the Cornerstone Performance Management System. (2011.HC.4.4A)                              | <ul style="list-style-type: none"> <li>At the end of FY11, the CFPB Performance Management system was chosen and early in FY12 the inCompass tool was implemented for CFPB personnel performance management.</li> <li>CFPB benchmarked Pay for Performance programs in similar federal and corporate environments.</li> <li>The Human Capital Strategic Plan FY13-FY15 has identified the need to reassess the compensation structure annually, and to benchmark competitor agencies and similar businesses in the market.</li> </ul>  | Closed                                 |
| CFPB should communicate a performance philosophy that creates incentives. (2011.HC.4.4B)   | <ul style="list-style-type: none"> <li>CFPB Human Capital Strategic Plan FY13-FY15 discusses the tactic to conduct year-one review of performance management strategy, policy and process to address the CFPB performance management needs and effectiveness; and revise and improve the program as needed.</li> <li>The CFPB performance program was implemented during the FY12 cycle. Incentives include pay and non pay incentives.</li> </ul>   | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| CFPB should develop a Diversity Plan and communicate the plan throughout CFPB. (2011.HC.4.5A, Risk of Deficiency or Noncompliance)  | <ul style="list-style-type: none"> <li>• Assessment and benchmarking of other agencies was used as an input to develop the Office of Minority and Women Inclusion.</li> <li>• CFPB Human Capital Strategic Plan FY13-FY15 describes assess the Bureau's organizational culture and develop a diversity and inclusion plan. Through performance evaluations, develop accountabilities for fostering and promoting a diverse, inclusive, and engaged workforce.</li> <li>• See demonstrated performance for 2011.HC.3.3B for additional details.</li> </ul>   | Closed                                 |
| CFPB should publish up-to-date policies that indicate zero tolerance for sexual harassment and discrimination in the workplace. (2011.HC.4.5B)  | <ul style="list-style-type: none"> <li>• CFPB developed a policy on Harassment and Inappropriate Conduct, which was communicated to all staff on December 11, 2011 through a memorandum from CFPB Deputy Director, Raj Date.</li> <li>• The CFPBedia wiki site contains information on the Bureau's Equal Opportunity Employment policies, and steps for reporting harassment and inappropriate conduct (including contact information).</li> <li>• See demonstrated performance for 2011.HC.3.3B for additional details.</li> </ul>  | Closed                                 |
| CFPB should develop a long-term Recruitment Plan to: address staffing needs and anticipated gaps in critical skills and competencies; establish performance indicators; and close skill gaps for mission-critical occupations. (2011.HC.5.1A) | <ul style="list-style-type: none"> <li>• OHC has developed a talent acquisition strategy, a methodology and approach for recruiting (including culture recruiting, progressive approaches, branding, events and development programs).</li> <li>• CFPB Human Capital Strategic Plan FY 13-FY15 establishes an objective to recruit and retain a high quality, diverse and engaged staff through effective workforce planning and talent acquisition methods, strong engagement, diversity, and inclusion programs, and a competitive total rewards package.</li> <li>• The workforce planning process is geared to assessing gaps in skills and competencies, and CFPB has identified mission-critical roles necessary for FY12.</li> <li>• While CFPB has accomplished a great deal in the area of talent acquisition, the Bureau should establish a process for meeting future/long term recruitment needs in a competitive environment.</li> <li>• See demonstrated performance for 2011.HC.2.1 and 2012.HC.2.3 for additional details.</li> </ul> | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| <p>CFPB should develop innovative hiring and outreach programs to attract talented and skilled candidates from diverse backgrounds. (2011.HC.5.1B)</p> | <ul style="list-style-type: none"> <li>• CFPB developed the Pathways hiring program policy to provide students with the opportunity to be exposed to the workings of the federal government and CFPB. The program is geared to interns, Presidential management fellows, and recent graduates. A Memorandum of Understanding (MOU) was established with OPM, to hire 220 new employees and seasonal interns during a two year period from 2012 to 2014.</li> <li>• To identify interns for the upcoming year, CFPB developed the Student Ambassador Program to employ select previous interns as ambassadors for high priority schools.</li> <li>• A hiring strategy has been developed to allow individuals to begin CFPB internships in their junior year of college, continue as a part-time extern during their senior year, and then have an opportunity to be hired into the CFPB workforce upon graduation. This strategy maximizes the hiring pipeline and minimizes risk.</li> <li>• CFPB has deputized over 70 staff as recruiters by outfitting them with branded recruiting materials to share with potential candidates (via multiple channels, including in-person, email and social networks).</li> <li>• An employee referral policy for mission critical and hard to fill positions is in development.</li> <li>• CFPB holds recruiting events and conducts outreach across the country, and engages the Bureau's Director and Deputy Director in events.</li> <li>• See demonstrated performance for 2011.HC.5.1A and 2011.HC.2.1 for additional details.</li> </ul> | <p>Closed</p>                          |
| <p>CFPB should develop a recruitment process that includes manager activities for recruitment within the manager's units. (2011.HC.5.1C)</p>           | <ul style="list-style-type: none"> <li>• CFPB begins during new employee orientation to discuss and enlist personnel in the recruitment process.</li> <li>• Some CFPB employees engage their personal network by using their LinkedIn account to advertise open positions at the Bureau. This provides leads that the talent acquisition team could not otherwise reach.</li> <li>• The talent acquisition team sends emails to staff, containing information about open positions.</li> <li>• See demonstrated performance for 2011.HC.2.1 for additional details.</li> </ul>   | <p>Closed</p>                          |
| <p>CFPB should explore strategies to retain personnel in mission-critical occupations. (2011.HC.5.2A)</p>  | <ul style="list-style-type: none"> <li>• See demonstrated performance for 2011.HC.3.3B for additional details.</li> </ul>  | <p>Closed</p>                          |
| <p>CFPB should develop a retention plan (2011.HC.5.2B)</p>   | <ul style="list-style-type: none"> <li>• CFPB Human Capital Strategic Plan FY13-FY15 discusses creation of an employee engagement program to provide the tools and processes necessary to facilitate and improve employee engagement across the Bureau.</li> <li>• CFPB has developed policies and instituted workforce flexibilities and other employee engagement programs and activities that will become part of CFPB retention program.</li> </ul>  | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| CFPB should develop a Human Capital Strategy that aligns with the Bureau's mission, goals and objectives, and facilitates workforce planning. (2011.HC.6.1A)  | <ul style="list-style-type: none"> <li>• The CFPB Human Capital Strategic Plan FY13-FY15 was approved October 2012. It aligns with CFPB mission, goals and objectives to implement the OHC processes and systems.</li> <li>• See demonstrated performance for 2011.HC.2.5 for additional details.</li> </ul>  | Closed                                 |
| CFPB should establish a strategic partnership with external Human Resources professionals, to enhance workforce planning. (2011.HC.6.1B)  | <ul style="list-style-type: none"> <li>• The CFPB Office of Human Capital collaborated with human resource professionals in federal agencies and corporate entities by benchmarking methods used to develop CFPB policies and strategic approaches for multiple human capital systems.</li> <li>• OHC established relationships with human resource consultants and vetted ideas across CFPB, including recruitment methods, staffing practices and plans.</li> <li>• Continuing efforts are planned in the CFPB Human Capital Strategic Plan to refine organizational charts, staffing and recruitment activities for workforce planning.</li> </ul> | Closed                                 |
| CFPB should develop a process to collaborate with other federal government agencies and private sector organizations regarding effective human capital strategies, and to benchmark best practices and lessons learned. (2011.HC.6.1C)  | <ul style="list-style-type: none"> <li>• CFPB has performed benchmarking against Federal agencies and private corporations for the development of multiple human capital policies, programs and plans. These activities have provided depth of information to develop policies, programs and plans for CFPB and its environment.</li> <li>• See demonstrated performance for 2011.HC.6.1B for additional details.</li> </ul>  | Closed                                 |
| CFPB should develop a formal accountability system that states the bureau's accountability policy, key responsibilities, outcomes and measures, milestones and results. The system should meet OPM's requirements for a sound human capital accountability system. (2011.HC.6.2A) | <ul style="list-style-type: none"> <li>• The CFPB Human Capital Strategic Plan FY 13-FY15 contains strategies and tactics to develop human capital infrastructure through creating human capital policies, improving human resource information systems, effectively allocating and prioritizing resources, and achieving desired human capital outcomes through mutual accountabilities.</li> <li>• Implementation of the CFPB Human Capital Strategic Plan – Project Plan will formalize the CFPB OHC program for FY13-FY15.</li> <li>• See demonstrated performance for 2011.HC.2.5 for additional details.</li> </ul>                             | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|--|--|--|
| CFPB should develop an appraisal system for senior executives that have appropriate measures or indicators of employee and/or customer feedback. (2011.HC.6.2B)                                      | <ul style="list-style-type: none"> <li>• As part of the CFPB Performance system, Rating Officials gather feedback from peers, customers, and subordinates for the year-end appraisal process. Employees offer their own perspective through self-assessment.</li> <li>• Review of this process is ongoing, as part of CFPB Human Capital Strategic Plan FY13-FY15, which states CFPB will continually assess, monitor and improve the performance system.</li> </ul> | Closed                                 |
| CFPB should develop a process that holds managers and human resources officers accountable for efficient and effective human resources management in support of the Bureau's mission. (2011.HC.6.2C) | <ul style="list-style-type: none"> <li>• The CFPB Human Capital Strategic Plan (Appendix D: Human Capital Accountability Design) illustrates the data sources initially identified as relevant to each of 10 Key Performance Indicators (KPI) recommended for review.</li> <li>• Tactic Z: Develop Human Capital accountability system to track and report on how the Bureau is meeting human capital objectives.</li> </ul>   | Closed                                 |

## Section 8: Information Technology

### 8.1 Scope of Audit

In FY11, the ASR Team evaluated CFPB’s performance in the area of Information Technology. Specifically, we examined the extent to which the Bureau had: (1) complied with relevant laws and regulations; (2) achieved organizational goals and objectives; and (3) aligned with industry best practices.

Our analysis in FY11 was guided by standards and criteria defined by the Federal IT Dashboard (FITD). The FITD is a standardized method for all federal agencies to report on the health of their major IT projects, and to support decisions regarding the investment and management of IT resources to determine whether existing IT investments are proceeding according to established plans with respect to scope, schedule, and budget. The second component of our analysis in FY11 evaluated the operations of the IT investment process. The purpose of this component was to evaluate the overall planning and control of the IT investment process, including the methods that CFPB used to select and manage IT projects, as well as the standards that were used to determine whether IT investments are supporting strategic goals. Finally, our analysis in FY11 evaluated the maturity of CFPB’s IT investment process using the standards and criteria that are defined by GAO’s Information Technology Investment Management (ITIM) Framework.

Based on the analysis conducted in FY11, we offered 28 recommendations and suggestions related to performance elements in the area of Information Technology. In addition, 4 recommendations and suggestions originally evaluated in the Consumer Response area were reassigned to the Information Technology review area for FY12 evaluation. Included on this list was a broad spectrum of items, ranging from specific corrective actions, to long-term strategic initiatives. The purpose of this FY12 performance audit is to: (1) evaluate the extent to which CFPB has addressed each of the recommendations and suggestions offered in FY11; and (2) provide new or updated recommendations for FY12, to address any residual performance gaps. These “residual recommendations” have been grouped based on severity into one of the categories defined in Section 1.3.3.

### 8.2 Findings and Recommendations

Based on the Bureau’s demonstrated performance, we assigned a status of “Closed” to 31 of the 32 FY11 recommendations and suggestions (97%), indicating that no formal corrective action is needed. Included among these closed items are 4 performance improvement opportunities, where suggestions are provided but no corrective action is required. The remaining item is classified as a risk of deficiency or noncompliance, which requires corrective action.

#### 8.2.1 Summary of Demonstrated Performance

Table 9 presents the following information for each of the significant performance issues and performance improvement opportunities contained in the FY11 report:

- **Recommendation Statement.** This column states the recommendation or suggestion that was provided in the FY11 Audit Report and provides a unique ID code for each.

- **Summary of CFPB Corrective Actions.** This column reports information about: (1) the actions that CFPB has taken to address the recommendation; (2) plans that CFPB has put in place to address the recommendation; and (3) the status of CFPB’s efforts to address the recommendation.
- **FY12 Status.** This column reports the ASR Team’s assessment of whether or not additional action is required to address the recommendation. A status of “no further action required” indicates that no further corrective action or monitoring is needed with respect to the recommendation—either because it has been achieved, or because the Bureau’s ongoing operational and management activities provide adequate control over the recommended action.

## 8.2.2 Significant Performance Issues

In this section, we identify residual recommendations and suggestions related to a performance issue from FY11 that requires further action. For this item, we document: (1) the categorization of the residual performance issue based on its FY12 severity; (2) the criteria, condition, cause, and effect associated with the performance issue; and (3) our recommendations for addressing the performance issue.

**2012.IT.3 COOP Development (Risk of Deficiency or Noncompliance).** Government-wide requirements related to Continuity of Operation Plan (COOP) development, operation and testing are principally outlined within: (i) Title III of the E-Government Act—entitled the Federal Information Security Management Act of 2002 (FISMA)—and accompanying standards promulgated by the National Institute of Standards and Technology (NIST), including Federal Information Processing Standards (FIPS) 199, FIPS 200, and NIST Special Publication (SP) 800-53; and (ii) Federal Continuity Directive 1, “Federal Executive Branch National Continuity Program and Requirements” (February 2008) or FCD 1, developed and published by the Department of Homeland Security in coordination with its interagency partners.

In our FY11 Performance Audit, we recommended that CFPB “[d]evelop and test a Continuity of Operations Plan (COOP) that is specific to CFPB, within the Treasury’s larger plan.” While some of the systems that CFPB uses are owned and managed by the Bureau of Public Debt, the National Finance Center, and Treasury Departmental Offices, the agency continues to expand its internally-managed IT infrastructure, in support of key operating units of the agency. The ongoing build-out of the CFPB’s internally-managed IT infrastructure expands the agency’s responsibility for COOP planning, coordination and management.

CFPB has begun a comprehensive COOP development effort, but planning and documentation are still in the initial stages. Moreover, CFPB has not yet completed an essential assessment and determination of the agency’s pre-defined Recovery Time Objective/Recovery Point Objective (RTO/RPO) for all major system, in accordance with FIPS 199, FIPS 200, and FCD 1. In the event of a significant interruption or disaster, the RTO/RPO objectives would guide critical decisions regarding communications, personnel, facilities, processes, and systems. The RTO/RPO also outlines the foundational assumptions for overall and detailed component-level COOP planning efforts, guiding preventive and responsive resource requirements under multiple disaster scenarios.

As near-term steps within the agency’s multi-year COOP plan development, we recommend the agency:

- 1) Formally assess, document and obtain approval for its business continuity and recovery RTO/RPO requirements for all major aspects of headquarter and regional operations, in accordance with applicable COOP standards;
- 2) Finalize pertinent policies essential for the viability of COOP planning (e.g., Occupant Emergency Plan); and
- 3) Continue to flesh-out the COOP documents and component plans, based on the approved business continuity and recovery RTO/RPO requirements.

**Agency Response.** The Bureau concurs with this recommendation and is in the process of developing a COOP. Since the Bureau began operations, it has utilized the Department of the Treasury, the Bureau of Public Debt, and National Finance Center technology platforms, which already have robust backup and disaster recovery planning to ensure continuity for the Bureau's critical system operations. In addition, the Bureau is moving forward with the development of its COOP and, in the meantime, has implemented a number of contingency processes to facilitate continuity of operations in the event of a significant interruption or disaster. As noted in the Summary of CFPB Actions, the Bureau has policies in place regarding the Telework Program and Alternative Work Schedules, which provide CFPB employees with remote access to Bureau resources. Furthermore, the Bureau's key systems are backed up and are able to be reconstituted in the event of a disaster or significant outage. The Bureau has documented an IT contingency planning strategy prioritizing this reconstitution of its systems.

### 8.2.3 Performance Improvement Opportunities

Below, we present information on aspects of performance related to FY11 performance issues that we believe could be improved, but do not require corrective action. For each of these performance improvement opportunities, we offer suggestions for future action, and we summarize the criteria on which these suggestions are based.

**2012.IT.1 E-Government Act of 2002 Annual Report.** The CFPB Legal Division recently determined the applicability of the E-Government Act of 2002 (EGOV) where the EGOV Act requires each agency to compile and submit to OMB an annual EGOV Report on a) the status of the implementation by the agency of electronic government initiatives; b) compliance by the agency with the EGOV Act; and c) how EGOV initiatives of the agency improve performance in delivering programs to constituencies. CFPB's planning and implementation activities for the initial EGOV Report are at their inception. We recommend the CIO lead the agency's EGOV Act implementation efforts to ensure timeliness and consistency with the OMB reporting requirements.

**2012.IT.2 IRB Governance.** The Investment Review Board (IRB) is an essential governance function of the agency—responsible for ensuring that significant investments, which could span multiple years, are effectively aligned with the agency's mission and carefully managed to achieve the expected returns. CFPB continues its efforts to expand the capability of its IRB, which we encourage and support. To enhance the operation of the IRB, we recommend the IRB:

- 1) Build a database repository to gather, manage, track and report all investment requests;
- 2) Seek to have new investment cases segmented into components with discrete milestone progress points, as a means to improve tracking and management;

- 3) Increase agency-wide training and awareness to improve the depth and quality of ROI input data for future investment cases; and
- 4) Expand its meetings to include review of “in flight” investments previously approved, closely evaluating progress and achievement of planned ROI.

**2012.IT.4 Data Coordination Council.** A Data Coordination Council has been formed within the Bureau, and approved for one-year of work by the Operations and Advisory Committee (OAC). The Council began its work in December 2011 and continues its efforts to provide enterprise-wide data governance, policy, processes, architecture and tools. We recommend the OAC extend the duties of the Council which are directly aligned to the strategy of the CFPB in being a data-driven agency. We recommend the Council develop an Enterprise Data Strategy to establish a unifying vision and roadmap for the agency to achieve its strategic goal.

**2012.IT.5 Website Usability and Experiential Testing.** CFPB has tested certain key areas of its website, the most formal of which are: “Know Before You Owe,” where the Bureau met with consumers in six cities to obtain feedback; and, the consumer experience training program, starting with home ownership and then paying for college, where CFPB engaged a contractor to do up-front research work to see how the online courses would be most effective. However, much of the usability and experiential testing is currently performed by internal agency resources. Given the significant emphasis the agency has placed on its website presence for consumer complaint submission, education and awareness, resource materials, and access to CFPB information, we recommend the Digital Media Team expand its efforts by having comprehensive usability and experiential tests of its website periodically performed by objective, external contract resources.

**Table 9: Actions Taken by CFPB to Address Recommendations from the FY11 Audit Report**

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| Continue with plans to improve the website and further develop CIS. (2011.IT.1.1A)  | <ul style="list-style-type: none"> <li>• A team has been organized within CFPB (comprising members from the Office of Consumer Education and Technology &amp; Innovation [T&amp;I]) to provide a governance structure for website content. The team is led by a unit leader within Office of Consumer Engagement and the CIO co-chairs this group.</li> <li>• The initial version (v1.0) of the CFPB website, <a href="http://www.consumerfinance.gov">www.consumerfinance.gov</a>, was launched in February 2011. Subsequent major releases were published in July 2011 (v2.0) and February 2012 (v3.0).</li> <li>• To enhance the functionality and usability of the website, the following enhancements have been launched or are planned for the near future:                             <ul style="list-style-type: none"> <li>○ With the v3.0 release, CFPB revamped the structure and navigation of the website offering more intuitive menu tabs: "Inside the CFPB," "Get Assistance," "Participate," "Regulation," and "Submit a Complaint;"</li> <li>○ The "Ask CFPB" participatory knowledgebase and frequently asked questions (FAQ) is easily accessed under the "Get Assistance" tab on the website's main menu;</li> <li>○ Syndicated feeds from the "Ask CFPB" FAQ are being evaluated to broaden the access to published information; and</li> <li>○ General site-wide search functionality was released in August 2012.</li> </ul> </li> <li>• CFPB is now using WordPress as its primary Content Management System (CMS), offering greater web platform functionality and developer toolsets. CFPB also uses the Django programming framework to create most of its interactive, data-driven applications.</li> <li>• CE and T&amp;I are also partnering to create a robust customer experience platform, centering around consumers' key financial life goals. The first module, Paying For College, was successfully beta tested in April, and another iteration will be released this Fall.</li> </ul> | Closed                                 |
| Develop performance measures for e-Government that are: (1) citizen-centric; (2) productivity related; and (3) linked to the CFPB's Strategic Plans. (2011.IT.1.1B) | <ul style="list-style-type: none"> <li>• T&amp;I has been an active participant in the CFPB GPRA-MA planning and implementation efforts. T&amp;I participation will continue as the agency goals, performance measures and targets are formalized and published to the public.</li> <li>• On-going evaluation is being performed of various performance measurement methods and toolsets.</li> </ul>  | Closed                                 |
| Conduct Privacy Impact Assessments for all applicable IT systems. (2011.IT.1.1C)  | <ul style="list-style-type: none"> <li>• PIAs have been completed satisfactorily for all systems and may be found at <a href="http://www.consumerfinance.gov/privacy-office/">http://www.consumerfinance.gov/privacy-office/</a>.</li> <li>• The T&amp;I PMO has incorporated security and privacy templates into the standard set of artifacts to be completed at the onset of each IT project. This is a proactive attempt to assure PIAs are completed prior to development.</li> </ul>  | Closed                                 |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations   |
|--|---|--|
| Develop annual e-Government Report to Congress. (2011.IT.1.1D)   | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.IT.1.1B.</li> <li>In August 2012, the CFPB's Legal Division released its determination of applicability of the e-Government Act of 2002 to CFPB.</li> <li>The CIO and T&amp;I staff are beginning planning efforts to fully-implement the adopted portions of the e-Government Act, including assigning accountability and reporting responsibilities within T&amp;I.</li> </ul>  | Additional Action Suggested<br><br>2012.IT.1 (Performance Improvement Opportunity): We recommend the CIO lead the agency's EGOV Act implementation efforts to ensure timeliness and consistency with the OMB reporting requirements. |
| Implement annual FISMA audits. (2011.IT.1.1E)  | <ul style="list-style-type: none"> <li>The Board of Governors of the Federal Reserve – Office of Inspector General (OIG) continues to monitor and report on the CFPB's efforts in establishing an information security program.</li> <li>The OIG performed a comprehensive FISMA audit and reported its results November 15, 2011, and has commenced another cycle of its FISMA audit for FY12 (to include an assessment of the Consumer Response website).</li> <li>It is anticipated that GAO will also undertake some evaluation of the CFPB core financial and operational systems as part of its annual financial statement audit.</li> </ul>  | Closed   |
| Establish policies and procedures to support the detection, assessment, and mitigation of risks that could result from unauthorized or inappropriate use of organizational information. (2011.IT.1.1F)   | <ul style="list-style-type: none"> <li>CFPB has created a security program to protect against unauthorized system access. This performance of this program was audited in 2011.</li> <li>The Office of the Chief Financial Officer (OCFO) is principally charged with facilitating the agency-wide risk management plans, actions, and progress reports.</li> <li>T&amp;I plans to adopt OCFO protocols for any IT-centric risks (e.g., continuity of operations [COOP], information security, privacy), including any "risk register" that might be developed.</li> <li>Since CFPB leverages core systems from the Treasury – Bureau of Public Debt (BPD), the agency is subject to certain BPD policies and procedures, notably in the areas of information security risk detection, assessment, and mitigation.</li> <li>The T&amp;I Program Management Office (PMO) has incorporated "issues and risks" tracking within its standard Project Reporting output documents.</li> </ul> | Closed   |
| Stand up a formal Program Management Office for CFPB Information Technology. Implement a portfolio approach to IT investment management, including analysis of returns on each investment. (2011.IT.1.2) | <ul style="list-style-type: none"> <li>The T&amp;I Program Management Office (PMO) has been operating for over one year and a Director was recently appointed to lead the PMO.</li> <li>The PMO function has evolved from a year ago, presently staffed predominantly with government employees. The PMO is nearly fully staffed with 5 Technology Portfolio Managers (TPM) (1 vacancy), 2 Business Analysts, 3 Project Managers (1 to on-board soon), 1 IT Investment Manager (to on-board soon), and 1 Product Director for Finance Education.</li> <li>T&amp;I PMO has briefed either the Executive Committee, Policy Committee and/or Operations Advisory</li> </ul>  | Closed   |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations   |
|---|---|--|
|   | <p>Committee (OAC) at least three times pertaining to the PMO development, function and progress.</p> <ul style="list-style-type: none"> <li>• Information has been shared throughout the Bureau to explain the T&amp;I PMO “work in-take” process for new projects.</li> <li>• To help to avoid rogue projects, portfolio managers are plugged into demand of business units. The PMO also works in close concert with CFPB procurement to head off any outlier initiatives.</li> <li>• A compendium of materials is used (e.g., requirements management, cost/schedule variance). These materials are subject to periodic review and revision to improve applicability and usefulness.</li> <li>• There are currently approximately 60 projects in the T&amp;I project portfolio being managed and monitored by the PMO with an additional 60 in the backlog queue.</li> <li>• Weekly PMO meetings are held to review all projects “in flight” and to manage resources, new resource requests, and new project in-take screening. The first of these weekly PMO meetings was held starting October 2011.</li> <li>• Project Management methodologies (both for hybrid and agile project life cycles) continue to be refined for use by the agency.</li> <li>• CFPB plans to implement JIRA as its enterprise program / project management toolset to help enable the PMO methodologies and related artifact templates.</li> <li>• By Fall 2012, the PMO plans to migrate the storage of project artifacts from a shared network drive to a Microsoft SharePoint environment – organized by line of business. With the migration, refined PMO artifact templates will be propagated for use along with automating the “work in-take” form for enhanced reporting.</li> </ul> |  |
| <p>Continue to identify meaningful IT investments and use the established IRB process to select and track the IT investments. (2011.IT.1.3)</p> | <ul style="list-style-type: none"> <li>• CFPB has had a functioning IRB since approximately February 2011. Effective during the Fall 2011 following a study conducted by an outside strategy firm, CFPB moved primary responsibility for managing the IRB from T&amp;I to the OCFO. The effect was that all agency investments were evaluated, not solely those involving T&amp;I resources. The IRB is currently chaired by the CFO. Broad representation from across the agency makes up the IRB membership.</li> <li>• Agency investments exceeding \$500,000 in contractual services or external costs for a single budget year (or exceeding \$2.5 million over 5 or more years) are subject to IRB in-take and review. The IRB chair also has discretion to request smaller investments be brought to the IRB for review.</li> <li>• The IRB process conforms to major aspects of the federal Capital Planning and Investment Control (CPIC) process.</li> <li>• The IRB meets as needed and as investment business cases are generated. For Budget Year 2014, CFPB began to evaluate investments during the formulation of the agency's budget. Over 70 investments were identified for review. Eventually, CFPB plans to perform periodic “check-in” reports</li> </ul>   | <p>Additional Action Suggested</p> <p>2012.IT.2 (Performance Improvement Opportunity): to enhance the operation of the IRB, we recommend the IRB:</p> <ol style="list-style-type: none"> <li>1) Build a database repository to gather, manage, track and report all investment cases;</li> <li>2) Seek to have new investment cases segmented into components with discrete milestone progress points as a means to improve</li> </ol> |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations  |
|--|---|---|
|  | <p>(by investment) prepared during the course of each investment life cycle.</p> <ul style="list-style-type: none"> <li>• An IRB charter has been published and standardized “smart forms” are used to capture factors such as investment identifier, investment information, ROI analyses, and risks and mitigation plans. CFPB plans to build a database repository for all investment cases to improve management, tracking and reporting.</li> <li>• A T&amp;I IT Investment Manager has been hired and charged with overseeing major IT investments approved by the IRB.</li> <li>• CFPB non-pay expenditures are not approved for payment under the Budget Control Sheet process unless the IRB has approved the investment case.</li> </ul>  | <p>tracking and management;</p> <p>3) Increase agency-wide training and awareness to improve the depth and quality of ROI input data for future investment cases; and</p> <p>4) Expand its meetings to include review of “in flight” investments previously approved, closely evaluating progress and achievement of planned ROI.</p> |
| <p>Continue the IRB process and add a PMO component to manage cost and scheduling information on a standardized basis. Consider employing Earned Value Management (EVM) or other project management metrics as needed as the organization grows. (2011.IT.1.4)</p> | <ul style="list-style-type: none"> <li>• Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> <li>• At a high level, both cost and schedule variances are currently managed by a) weekly PMO meetings to discuss project status, and b) project team meetings held as needed.</li> <li>• With the introduction of JIRA as an enterprise program / project management tool, CFPB will further standardize task and schedule tracking for enhance variance reporting.</li> <li>• Budget and cost variance tracking will continue to evolve as both the IRB and PMO continue to prescribe standardized estimating at the inception of an investment or project’s life cycle. It is anticipated the agency will initially focus its efforts on significant investments / projects.</li> </ul> | <p>Closed</p>   |
| <p>The IT organization should continue to add appropriate staff to maintain a ratio of between 8% to 10% as compared to the total staff of CFPB. (2011.IT.2.1)</p>   | <ul style="list-style-type: none"> <li>• By the end of FY12, T&amp;I anticipates being near its approved staffing level. Additional contractor support brings T&amp;I staffing to within the 8%-10% range of total CFPB staffing.</li> <li>• On-going interaction occurs frequently between the CIO’s Chief of Staff and the Chief Human Capital Officer (CHCO) to assure staffing levels are aligned with the agency’s strategic plans and operating budgets.</li> </ul>   | <p>Closed</p>   |
| <p>The IT organization should continue to increase its network capacity. (2011.IT.2.2A)</p>  | <ul style="list-style-type: none"> <li>• Approved by the IRB, CFPB has undertaken a major capital investment to expand its wide-area network (WAN), supported also by increased bandwidth.</li> <li>• The General Services Administration (GSA) is assisting with the procurement; award(s) are anticipated by September 2012. WAN enhancements will likely begin before the end of calendar year 2012.</li> <li>• The agency’s intent to drive more video collaboration coupled with expanding data management and analytics needs are driving factors for this investment. A significant amount of growth was built into</li> </ul>   | <p>Closed</p>   |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions   | FY12 Status / Residual Recommendations   |
|--|---|--|
| <p>The IT organization should develop and test a Continuity of Operations Plan (COOP) that is specific to CFPB, within the Treasury's larger plan. (2011.IT.2.2)</p> | <p>the future WAN plans to try to stay ahead of agency needs.</p> <ul style="list-style-type: none"> <li>• Outlines for a COOP document and Information Technology Contingency Planning Process have been drafted.</li> <li>• Various CFPB policies have been developed, including: Alternative Work Schedules Policy, Telework Program Policy, External Threats to Personnel and Property Policy (draft), and Occupant Emergency Plan (draft).</li> <li>• Safety and preparedness training presentations have been made to volunteer floor wardens.</li> <li>• A former US Treasury COOP planner has been hired by CFPB to build out the agency's plans.</li> <li>• The agency plans to acquire a Mass Notification System to help alert and broadcast emergency notices to personnel and other affected parties.</li> </ul> | <p>Additional Action Required</p> <p>2012.IT.3 (Risk of Deficiency or Noncompliance): We recommend the agency:</p> <ol style="list-style-type: none"> <li>1) Formally assess, document and obtain approval for its business continuity and recovery RTO/RPO requirements for all major aspects of headquarter and regional operations, in accordance with applicable COOP standards;</li> <li>2) Finalize pertinent policies essential for the viability of COOP planning (e.g., Occupant Emergency Plan); and</li> <li>3) Continue to flesh-out the COOP documents and component plans, based on the approved business continuity and recovery RTO/RPO requirements.</li> </ol> |
| <p>The IT organization should formalize an organizational taxonomy and enterprise data dictionary. (2011.IT.2.3)</p>   | <ul style="list-style-type: none"> <li>• CFPB is in the process of hiring a Chief Data Officer (CDO). Currently, the T&amp;I Data Team Lead is acting as the CDO.</li> <li>• A Data Coordination Council DCC has also been formed, chaired by the CDO, to vet agency-wide data sourcing, ownership and control needs. Where necessary, this Council forms working groups to coordinate specific needs and requirements.</li> <li>• The Data Team has also begun a metadata management project to create a "data governance" protocol and taxonomy across the agency which will include an inventory of all datasets and corresponding data dictionaries. Accelerated progress is expected with the appointment of the CDO.</li> </ul>   | <p>Additional Action Suggested</p> <p>2012.IT.4 (Performance Improvement Opportunity): We recommend the OAC extend the duties of the Council which are directly aligned to the strategy of the CFPB in being a data-driven agency. We recommend the Council develop an Enterprise Data Strategy to memorialize a unifying vision and roadmap for the</p>   |

| FY11 Recommendation Statement<br>(ID#, Category)   | Summary of CFPB Actions  | FY12 Status / Residual Recommendations   |
|--|--|--|
|  |  | agency to achieve its strategic goal.  |
| The IT organization should formalize project artifacts per what is typically found in a PMO. (2011.IT.2.4)   | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.IT.1.2.</li> </ul>   | Closed   |
| The IT organization should perform formal user testing of the public-facing websites once the sites are more mature. This should include heat maps, usability tests, click counts, etc. (2011.IT.2.5)  | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.IT.1.1A.</li> <li>Ownership for public-facing website performance and usability, including testing, is jointly shared between the Office of Consumer Engagement and the T&amp;I team. A Digital Media Team has been organized within CFPB comprising members from the Office of Consumer Engagement and T&amp;I, and to provide a governance structure for website content.</li> <li>Some discrete testing work also has been performed by the Consumer Response team. For example, in one instance, students were active participants in CFPB's efforts to drive greater usability of the student loan content on the website. CFPB also has tested certain key areas of the website, the most formal of which are: "Know Before You Owe," where the Bureau met with consumers in six cities to obtain feedback; and, the consumer experience training program, starting with home ownership and then paying for college, where CFPB engaged a contractor to do up-front research work to see how the online courses would be most effective.</li> <li>CFPB has also, on a few occasions, leveraged the GSA laboratory environment to observe user interaction with various government systems.</li> <li>CFPB has expanded use of web traffic analytics tools to gauge the effectiveness of posted content.</li> <li>Starting with the v3.0 release of the website, CFPB has maintained a track changes log for revisions.</li> <li>CFPB acknowledges that with the increased maturity of the agency's website content, now is the appropriate time to externally validate the internal efforts to improve its usability. CFPB further acknowledges that any such usability testing must be regular and on-going. The agency anticipates releasing requirements to the contractor community in the Fall 2012 to contract for these services.</li> </ul> | Additional Action Suggested<br>2012.IT.5 (Performance Improvement Opportunity): Given the significant emphasis the agency has placed on its website presence for consumer complaint submission, education and awareness, resource materials, and access to Bureau information, we recommend the Digital Media Team expand its efforts to perform periodic external usability and experiential tests of its website products. |
| FY11 Executive Summary Recommendation – CFPB's IT investment management process is operating at "stage two" of the five-stage maturity model defined by the GAO's ITIM Framework. In order to progress to stage three, CFPB should build upon existing IRB processes, with an emphasis on: (1) | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.3 and 2011.IT.1.4.</li> </ul>  | Closed   |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| <p>grouping similar investments together and developing an IT portfolio; (2) creating and maintaining portfolio selection criteria; (3) examining the merits of each IT investment in the context of the portfolio; and (4) using an Enterprise Architecture to help align IT investments with strategic objectives. (2011.IT.2.6)</p>  |   |  |
| <p>The IRB was established very early in the CFPB organizing process. It has met weekly in order to address critical and fast moving needs. As the organization matures, the IRB should: (1) adopt a portfolio approach to IT investment management; (2) develop formal metrics and standards for project scoring and selection; and (3) retain consistent performance data. The portfolio approach will be needed to support budget formulation going forward. (2011.IT.3.1)</p>   | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.3 and 2011.IT.1.4.</li> </ul> | <p>Closed</p>                          |
| <p>The IT organization maintains project control through spreadsheets and various reporting artifacts (e.g., slides for IRB). As the organization matures, a "PMO-lite" approach is recommended to standardize project artifacts, provide a central portal to retain project artifacts, formalize cost and schedule variance reporting, and establish standardized metrics typical of a mature project management approach. The IRB process should have detailed documentation and supporting policy that dovetails with the PMO. (2011.IT.3.2)</p> | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul> | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions   | FY12 Status / Residual Recommendations |
|---|---|--|
| <p>In addition to the ad hoc After Action Reviews (AAR) that the IT organization currently performs, standardized and regularly scheduled reviews are recommended. This will be facilitated by establishing the PMO function and project management portal that will capture data needed for the reviews. This is highly recommended as major projects complete the implementation phase (first releases). Post Implementation Review (PIR) should become an IRB agenda item. (2011.IT.3.3)</p> | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>               | <p>Closed</p>                          |
| <p>Development of a standardized approach for communicating and tracking potential risks and mitigation strategies would be beneficial. This should focus on a "risk register" approach and ultimately feed a project database. (2011.IT.4.1)</p>   | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.1F, 2011.IT.1.3 and 2011.IT.1.4.</li> </ul> | <p>Closed</p>                          |
| <p>As the organization grows, a tool or methodology should be used to standardize the approach to requirements management. (2011.IT.4.2A)</p>   | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>               | <p>Closed</p>                          |
| <p>Requirements should be baselined at major project milestones. Baselined requirements should be used for testing and to monitor scope variance. (2011.IT.4.2B)</p>  | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>               | <p>Closed</p>                          |
| <p>As the organization matures, project requirements should be traced upward to organizational capabilities, in order to demonstrate alignment with CFPB strategy. (2011.IT.4.2C)</p>   | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>               | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
| <p>The contractor oversight function is primarily performed at the project level, with summary reporting to the IRB. As the organization grows, a uniform evaluation mechanism will be appropriate. (2011.IT.4.3)</p>   | <ul style="list-style-type: none"> <li>Where significant contractor support is required, IRB in-take, review and approval is a prerequisite. Following IRB approval, contractor services are procured through close interaction with the Office of Procurement.</li> <li>Contracting Officer Representatives (CORs) are designated within each contract award and possess technical proficiency to oversee and monitor contractor performance. CORs also routinely participate in IRB events to present information pertaining to the planned investment.</li> </ul> | <p>Closed</p>                          |
| <p>Since the organization was recently formed, historical performance has not been available or necessary. Lessons learned have been documented in After Action Reports. Going forward, additional structure will be required in order to establish performance metrics, develop analytical methods, and internalize lessons learned across the organization. (2011.IT.4.4)</p> | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>  | <p>Closed</p>                          |
| <p>CFPB IT has been growing rapidly to address the needs of the new organization. Skills and experience of the current staff are appropriate for the age of the organization. Key positions have been filled. Additional staffing is recommended to address CFPB growth and Portfolio and PMO needs. (2011.IT.4.5)</p>  | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>  | <p>Closed</p>                          |
| <p>Cost variance is understood and managed by the organization. Going forward, this component should be monitored and managed by a PMO organization in order to apply a uniform framework and collect historical performance data. EVM or other project management metrics may be needed as the organization grows. (2011.IT.4.6)</p>   | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>  | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
| <p>Schedule variance is understood and managed by the organization. Going forward, this component should be monitored and managed by a PMO in order to apply a uniform framework and collect historical schedule variance data. (2011.IT.4.7)</p> | <ul style="list-style-type: none"> <li>Refer to comments in Items 2011.IT.1.2 and 2011.IT.1.3.</li> </ul>  | <p>Closed</p>                          |
| <p>Bureau should monitor user comments for [website] navigational ease/utility; can leverage low cost existing tools to get general experience feedback (e.g., 4Q). (2011.CR.11.9 (CR45.4))</p>   | <ul style="list-style-type: none"> <li>Refer to comments in Item 2011.IT.2.5.</li> <li>Ownership for public-facing website performance and usability, including testing, is jointly shared between the Office of Consumer Engagement and the T&amp;I team. A Digital Media Team has been organized within CFPB (comprising members from the Office of Consumer Engagement and T&amp;I) to provide a governance structure for website content.</li> <li>Some discrete testing work also has been performed by the Consumer Response team. For example, in one instance, students were active participants in CFPB's efforts to drive greater usability of the student loan content on the website. CFPB also has tested certain key areas of the website, the most formal of which are: (1) "Know Before You Owe," where the Bureau met with consumers in six cities to obtain feedback; and (2) the consumer experience training program, starting with home ownership and then paying for college, where CFPB engaged a contractor to do up-front research work to see how the online courses would be most effective.</li> <li>CFPB has also, on a few occasions, leveraged the GSA laboratory environment to observe user interaction with various government systems.</li> <li>CFPB acknowledges that with the increased maturity of the agency's website content, now is the appropriate time to externally validate the internal efforts to improve its usability. CFPB further acknowledges that any such usability testing must be regular and on-going. The agency anticipates releasing requirements to the contractor community in Fall 2012 to contract for these services.</li> </ul> | <p>Closed</p>                          |
| <p>Bureau should consider moving "Building the CFPB" placement as functionality expands, to make room for clear calls-to-action associated with critical complaint intake activity. (2011.CR.11.10 (CR46.1))</p>                                  | <ul style="list-style-type: none"> <li>The Digital Media Team provides a governance structure for website content. The team is led by a unit leader within Office of Consumer Engagement and the CIO co-chairs this group.</li> <li>The initial version (v1.0) of the CFPB website, <a href="http://www.consumerfinance.gov">www.consumerfinance.gov</a>, was launched in February 2011. Subsequent major releases were published in July 2011 (v2.0) and February 2012 (v3.0).</li> <li>To enhance the functionality and usability of the website, the following enhancements have been launched or are planned for the near future:                         <ul style="list-style-type: none"> <li>With the v3.0 release, CFPB revamped the structure and navigation of the website offering more</li> </ul> </li> </ul>   | <p>Closed</p>                          |

| FY11 Recommendation Statement<br>(ID#, Category)  | Summary of CFPB Actions  | FY12 Status / Residual Recommendations |
|---|--|--|
|   | intuitive menu tabs: "Inside the CFPB," "Get Assistance," "Participate," "Regulation," and "Submit a Complaint;" <ul style="list-style-type: none"> <li>○ The "Ask CFPB" participatory knowledgebase and frequently asked questions (FAQ) is easily accessed under the "Get Assistance" tab on the website's main menu;</li> <li>○ Syndicated feeds from the "Ask CFPB" FAQ are being evaluated to broaden the access to published information; and</li> <li>○ General site-wide search functionality is planned for release in October 2012.</li> </ul> <ul style="list-style-type: none"> <li>● CFPB is now using WordPress as its primary Content Management System (CMS), offering greater web platform functionality and developer toolsets.</li> </ul> |  |
| Bureau should consider reducing height of the homepage to minimize vertical scrolling (2011.CR.11.11 (CR46.2))  | <ul style="list-style-type: none"> <li>● Refer to comments in 2011.IT.2.5.</li> </ul>  | Closed                                 |
| Bureau should consider modifying text included in images on the CFPB homepage; images cannot be read by search engines (Google, Yahoo, Bing) therefore, rank lower in search results (2011.CR.11.12 (CR46.3)) | <ul style="list-style-type: none"> <li>● Refer to comments in 2011.IT.2.5.</li> </ul>  | Closed                                 |

## Appendix A: List of CFPB Officials who Provided Input

| Operational Area                | CFPB Officials who Provided Input to this Audit   |
|---------------------------------|---|
| Budget                          | Steve Agostini<br>Ethan Bernstein<br>Zoe Berry<br>Adam Bunch<br>Andrew Feinberg<br>Laura Gulla<br>Lauren Hassouni<br>Dana James<br>Sheryl Kidd<br>Amanda Logan<br>Alicia McDonald<br>Althea Proctor<br>Darlene Riley<br>Jack Roziner<br>Freddie Velez<br>Brian Winseck  |
| Communications and Transparency | Camille Busette<br>Rohit Chopra<br>David Dubois<br>Laura Gulla<br>Lauren Hassouni<br>Gail Hillebrand<br>Jen Howard<br>Stephen Hunter<br>Peter Jackson<br>Wendy Kamenshine<br>Stacy Kane<br>Lisa Konwinski<br>Zixta Martinez<br>Martin Michalosky<br>Alicia McDonald<br>Matthew Pippin<br>Nick Rathod<br>Jeffrey Riley<br>Jeff Swartz<br>Chris Vaeth |
| Consumer Response               | Darian Dorsey<br>Kay Godette<br>Lauren Hassouni<br>Christopher Johnson<br>Lisa Lauroesch<br>Angela Martin<br>James McCarthy<br>Alicia McDonald<br>Judith Ochs<br>Scott Pluta<br>Deborah Reilly<br>Kathleen Zadareky   |

| Operational Area       | CFPB Officials who Provided Input to this Audit  |
|------------------------|--|
| Human Capital          | Ethan Bernstein<br>Libby Buechler<br>Marilyn Dickman<br>Laura Gulla<br>Lauren Hassouni<br>Dennis Slagter<br>Mary Tamberrino  |
| Information Technology | Steve Agostini<br>Lydia Barron<br>Zoe Berry<br>Zachary Brown<br>Adam Bunch<br>Matt Burton<br>Rachael Goldfarb<br>Lauren Hassouni<br>Stacy Kane<br>Norm Livingston<br>Amanda Logan<br>Alicia McDonald<br>Daniel Munz<br>Jack Roziner<br>Tammy Saiko<br>Joy Salazar<br>Michael Scarbrough<br>Claire Stapleton<br>John Steimke<br>Doug Taylor<br>Suzanne Tosini<br>Chris Willey |
| Privacy                | Zoe Berry<br>Zachary Brown<br>Adam Bunch<br>Hoa Crews<br>Wesley Fravel<br>Joshua Galicki<br>Laura Gulla<br>Stacy Kane<br>Chris Lambeth<br>Alicia McDonald<br>Shawn Mewhorter<br>Martin Michalosky<br>Sang Nahm<br>Sean Oakley<br>Nelly Ramdass<br>Jack Roziner<br>Joy Salazar<br>Claire Stapleton<br>Chris Willey  |

| Operational Area | CFPB Officials who Provided Input to this Audit  |
|------------------|--|
| Travel Policy    | Steve Agostini<br>Zoe Berry<br>Regina Braham<br>Adam Bunch<br>Edwin Chow<br>John Farrell<br>Laura Gulla<br>Lauren Hassouni<br>Dana James<br>Neil Kwatinetz<br>Alicia McDonald<br>Darlene Riley<br>Jack Roziner<br>Christina Whitty |

## Appendix B: List of Acronyms

|       |  |
|-------|--|
| AAR   | After Action Reviews                                     |
| AICPA | American Institute of Certified Public Accountants, Inc. |
| A/OPC | Agency/Organization Program Coordinator                  |
| ASR   | ASR Analytics, LLC                                       |
| ATM   | Automated Teller Machine                                 |
| BPD   | Bureau of Public Debt                                    |
| CAB   | Consumer Advisory Board                                  |
| CBA   | Centrally Billed Accounts                                |
| CDO   | Chief Data Officer                                       |
| CE&E  | Consumer Education and Engagement                        |
| CFO   | Chief Financial Officer                                  |
| CFPA  | Consumer Financial Protection Act                        |
| CFPB  | Consumer Financial Protection Bureau                     |
| CHCO  | Chief Human Capital Officer                              |
| CICA  | Canadian Institute of Chartered Accountants              |
| CIO   | Chief Information Officer                                |
| CIS   | Consumer Information System                              |
| CMS   | Content Management System                                |
| COO   | Chief Operating Officer                                  |
| COOP  | Continuity of Operations Plan                            |
| COR   | Contracting Officer Representatives                      |
| CPIC  | Capital Planning and Investment Control                  |
| CR    | Consumer Response  |
| CRM   | Customer Relationship Management                         |
| CSR   | Contact Service Representative                           |
| DASOD | Deputy Assistant Secretary of Defense                    |
| DCC   | Data Coordination Council                                |
| DOD   | Department of Defense                                    |
| ECC   | Excellence through Communication and Collaboration       |
| EEO   | Equal Employment Opportunity                             |
| EVM   | Earned Value Management                                  |
| FAQ   | Frequently Asked Questions                               |
| FDIC  | Federal Deposit Insurance Corporation                    |
| FISMA | Federal Information Security Management Act              |
| FMFIA | Federal Managers' Financial Integrity Act                |
| FOIA  | Freedom of Information Act                               |
| FTE   | Full-Time Equivalent                                     |
| FTR   | Federal Travel Regulation                                |
| GAGAS | Generally Accepted Government Auditing Standards         |

|         |  |
|---------|--|
| GAPP    | Generally Accepted Privacy Principles                    |
| GAO     | Government Accountability Office                         |
| GPRA    | Government Performance and Results Act                   |
| GPRA-MA | Government Performance and Results Act Modernization Act |
| GSA     | General Services Administration                          |
| HCAAF   | Human Capital Assessment and Accountability Framework    |
| HR      | Human Resources  |
| IBA     | Individually Billed Accounts                             |
| ICFR    | Internal Control over Financial Reporting                |
| IDP     | Individual Development Plan                              |
| IGA     | Office of Intergovernmental Affairs                      |
| ILSA    | Interstate Sales Full Disclosure Act                     |
| IRB     | Investment Review Board                                  |
| IT      | Information Technology                                   |
| ITIM    | Information Technology Investment Management             |
| KPI     | Key Performance Indicators                               |
| LOTA    | Limited Open Travel Authorization                        |
| MOU     | Memorandum of Understanding                              |
| OAC     | Operations and Advisory Committee                        |
| OCC     | Office of the Comptroller of the Currency                |
| OCFO    | Office of Chief Financial Officer                        |
| OHC     | Office of Human Capital                                  |
| OIG     | Office of the Inspector General                          |
| OIP     | Office of Information Policy                             |
| OJT     | On the Job Training                                      |
| OMB     | Office of Management and Budget                          |
| OPM     | Office of Personnel Management                           |
| PIA     | Privacy Impact Assessment                                |
| PII     | Personally Identifiable Information                      |
| PIR     | Post Implementation Review                               |
| PMO     | Program Management Office                                |
| PPP     | Policy, Procedure, and Process                           |
| PPT     | Policy and Procedure Team                                |
| PwC     | PricewaterhouseCoopers                                   |
| QA      | Quality Assurance  |
| QC      | Quality Control  |
| RACI    | Responsible, Accountable, Consulted, and Informed        |
| RMR     | Offices of Research, Markets, and Regulations            |
| ROI     | Return on Investment                                     |
| SLA     | Service Level Agreement                                  |
| SOP     | Standard Operating Procedure                             |
| SORN    | System of Record Notices                                 |

---

|      |                                      |
|------|--------------------------------------|
| TAF  | Travel Approval Form                 |
| T&I  | Technology and Innovation            |
| TPM  | Technology Portfolio Manager         |
| TTRA | Travel and Transportation Reform Act |
| WAN  | Wide Area Network                    |

---

## Appendix C: Audit Team

---

**Edward Hau** served as lead evaluator for **Communications and Transparency and Information Technology**. Mr. Hau has more than 24 years of global consulting experience, focused on regulatory consulting, operations, and technology risk management. He has led or managed over 40 SOX / OMB A-123 and internal audit engagements in both the commercial and public sector with a focus on IT audit readiness, risk assessment, and controls evaluation. Mr. Hau also has deep expertise in the delivery of OMB A-123, Appendix A, business process reengineering, and Federal financial management transformation services, and has helped clients yield clean opinions related to Internal Controls over Financial Reporting (ICFR).

**Michele Lebar** served as lead evaluator for **Human Capital and Organizational Development**. Ms. Lebar has more than 20 years of experience in organizational development and change management consulting, including leadership/talent development/coaching, succession planning, and performance management. Ms. Lebar's experience includes work with a variety of private sector industries, as well as extensive work with the Federal Government. Her recent work has included the design of a succession management training program for the Internal Revenue Service and the design of an organization development program for the Washington Metro Area Transit Authority. She holds a M.S. in Organizational Development from Johns Hopkins University.

**Shailendra (Shal) Malhotra** served as lead evaluator for **Budget Formulation and Execution and Travel Systems and Services**. Mr. Malhotra has significant experience in public accounting, financial management, consulting and contracting services for private industry and the U.S. federal government. He has a broad financial and performance management skill set and has over 11 years' experience providing advisory and support services to federal agencies. He coordinated the development and implementation of the Budget and Performance Management System (BPMS) for a comprehensive budget and performance integration program at USDA and has also led four projects at the U.S. Department of Health and Human Services. He has performed work for federal agencies in areas such as development of policies and procedures, risk management and process improvement, OMB Circular A-123 internal control, performance measurement and ABC costing, performance audits, financial oversight and compliance reviews, accounting operations, financial and accountability reporting, and other management projects.

**Bob Siegel** served as lead evaluator for **Privacy Programs, Policies, and Processes**. Mr. Siegel has more than 15 years of professional experience in the development of privacy policies and procedures, the definition of performance metrics to evaluate privacy maturity, and the evaluation of compliance with privacy policies. He is a Certified Information Privacy Professional, and has deep subject matter knowledge surrounding key laws and regulations surrounding consumer privacy and information security. Most recently, he served as Senior Privacy Specialist for a Fortune 500 consumer products company, where his responsibilities included the development of global privacy-related policies and procedures.

**Michael Stavrianos** served as **Project Manager** for this performance audit. Mr. Stavrianos has nearly 20 years of professional experience in the fields of project management, program evaluation, and requirements management. Over the past 13 years, he has managed a broad range of analytic consulting engagements for the Internal Revenue Service (IRS), including 5 years leading the development of business rules and requirements for various Business Systems Modernization programs. He has also led recent, large scale evaluations of operational performance for both the IRS and the Department of Defense. In addition, he has designed and administered customer surveys for numerous Federal agencies, and he has served as a subject matter expert on several analytical projects for the Department of the Treasury. He has been credentialed as a Project Management Professional (PMP) by the Project Management Institute.

**Melissa Toledo** served as lead evaluator for **Consumer Response**. Ms. Toledo has more than 15 years of professional experience including strategic planning, business analysis, program management, systems implementations, and market research. Her expertise in business planning and strategy implementation has achieved profound impacts on corporate efficiency and productivity. Ms. Toledo built and manages a department at a major U.S.-based professional services firm that uses market intelligence to better serve clients, improve competitive differentiation and maximize growth. She was instrumental in the development of the firm's first client loyalty measurement system and has also established several firm-wide performance initiatives that have resulted in significant improvements in client-experience ratings.

## **Appendix D: Agency Response**

---



Consumer Financial  
Protection Bureau

1700 G Street NW, Washington, DC 20552

November 13, 2012

Mr. Michael Stavrianos  
ASR Analytics, LLC  
1389 Canterbury Way  
Potomac, MD 20854

RE: Independent Performance Audit of CFPB Operations and Budget

Dear Mr. Stavrianos,

We have received a copy of your draft Independent Performance Audit of CFPB Operations and Budget, which fulfills the requirement that the Consumer Financial Protection Bureau (CFPB or Bureau) obtain an annual independent audit of its operations and budget (12 USC 5496a). We welcome the opportunity to review and comment on this draft report and appreciate the hard work and consideration of ASR Analytics, LLC (ASR) throughout the audit process.

For the fiscal year 2012 performance audit, ASR reviewed three key areas of operations: (1) Privacy Programs, Policies and Processes; (2) Travel Systems and Services and (3) the CFPB Budget. In addition, ASR evaluated the Bureau's actions to address the recommendations from the fiscal year 2011 performance audit, which focused on five key areas of operations: (1) Communications and Transparency; (2) Consumer Response; (3) Human Capital and Organizational Development; (4) Information Technology and (5) the CFPB Budget.

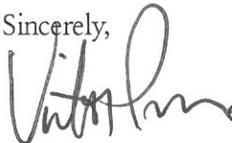
We appreciate ASR's recognition of the Bureau's progress toward addressing the recommendations from the fiscal year 2011 report. Ninety-nine percent of the 2011 recommendations and suggestions were deemed closed following ASR's evaluation. We are pleased to report that the Bureau's commitment and diligence toward strengthening operations have yielded such significant results.

The fiscal year 2012 report contains a number of helpful recommendations and performance improvement opportunities. Although we differ on the categorization of certain recommendations, we nevertheless appreciate that ASR has identified additional opportunities for performance enhancement. Continuous improvement in operations is a top priority for the Bureau and the Bureau is already implementing many of the actions noted in our responses. We will continue to address the report's recommendations and performance improvement opportunities over the coming year.

Thank you again for the opportunity to comment on the report. Any questions should

be directed to Stephen Agostini, Chief Financial Officer, at (202) 435-7942.

Sincerely,

A handwritten signature in black ink, appearing to read "Victor Prince". The signature is fluid and cursive, with a large initial "V" and a long, sweeping underline.

Victor Prince  
Chief Operating Officer

Enclosure

CFPB Responses to the Independent Performance Audit of CFPB Operations and Budget

**2012.PR.1.2 Establishment of a machine readable privacy notice on CFPB website (Noncompliance):** The E-Government Act of 2002 (EGOV) requires that privacy policies be present on agency web sites and that these policies be available in machine-readable format. The CFPB web-site currently contains high-level notices describing the CFPB Privacy Principles and references to SORNs for additional details, but these notices are not in machine-readable format. Without a machine-readable policy the privacy preferences set by visitors in their browsers will be ignored when CFPB's pages are rendered. We recommend that CFPB establish a machine readable privacy notice on its website.

**Agency Response:** The Bureau concurs with this recommendation and is in the process of determining how to satisfy the "machine readable privacy policy" requirement in a way that aligns with the Bureau's values of technology and user-friendly innovation. The Bureau's goal is to be in compliance with the requirement under the law.

As noted by ASR, the Bureau has a clear and easily accessible privacy policy posted on its website which informs users of the manner in which the Bureau handles privacy issues, including the use of cookies. The policy, per federal guidance, directs visitors to instructions on how to disable or modify their browser's acceptance of cookies. Like all modern sites, ConsumerFinance.gov respects a user's browser settings relative to how and when cookies should be accepted. Moreover, the CFPB website does not actively collect personally identifiable information (PII) without users' express consent; rather, users may choose to give consent and provide PII, as stated in CFPB policy. The Bureau has also published a Privacy Impact Assessment (PIA) about ConsumerFinance.gov. Therefore, there is little risk to consumers or others visiting ConsumerFinance.gov posed by the website's existing configuration at this time.

**2012.PR.2.3 Approval of CFPB Privacy Policy (Risk of Deficiency or Noncompliance):** OMB memorandum M-07-16 dated May 27, 2007 discusses agency responsibilities in protecting against the breach of personally identifiable information aiding in the protection of privacy. With regard to the establishment of policies for rules and consequences related to protecting personally identifiable information, Attachment 4, section A specifies:

*...it is the responsibility of each agency head to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.*

The Privacy Team has developed and communicated a Bureau-wide Privacy Policy for all CFPB systems and processes in alignment with applicable laws, regulations, and standards. While the current policy is awaiting final approval, the Privacy Team and others are operating as if approval has been achieved. We recommend that the formal approval process be completed for the Privacy Policy.

**Agency Response:** The Bureau's assessment is that this recommendation represents an opportunity for performance improvement and there exists no risk of deficiency or non-compliance. The only legally required policy related to privacy is the website privacy policy, which has been available from the time ConsumerFinance.gov went live. Under Section 1017(a)(4)(E) of the Consumer Financial Protection Act, the CFPB is generally not required to follow OMB guidance or consult with or obtain the approval of OMB with respect to Bureau affairs or operations. Therefore, the Bureau does not believe corrective action is required to mitigate the risk of future non-compliance or deficiency.

The Privacy Team is in the process of expanding and supplementing its program with additional policies and procedures to enhance the basic program, even though these are not legally required. Accordingly, the Privacy Team expects to finalize and implement both a Bureau-wide privacy policy and, in coordination with the Chief Information Security Officer, an acceptable use of technology policy in the normal course of operations.

**2012.PR.3.2 Bi-annual review of SORNs and PIAs (Risk of Deficiency or Noncompliance):** In accordance with GAPP privacy principles, the Bureau should provide notice about its privacy policies and procedures, and identify the purposes for which personal information is collected, used, retained, and disclosed. A high level privacy notice does appear on the CFPB website; the notice is written in clear, easy to understand language; and additional details are provided through SORNs and PIAs. However, there is no formal policy to revisit the SORNs and PIAs after the implementation of a system is complete. We recommend that all systems be reviewed at least bi-annually to identify any changes that may require changes to the notice.

**Agency Response:** The Bureau's assessment is that this recommendation represents an opportunity for performance improvement and there exists no risk of deficiency or non-compliance. The Privacy Team has plans to review and validate SORNs and PIAs every two years. Under Section 1017(A)(4)(e) of the Consumer Financial Protection Act, the CFPB generally is not required to follow OMB guidance or consult with or obtain the

approval of OMB with respect to Bureau affairs or operations, although the Bureau recognizes the procedures in Appendix I of OMB Circular A-130 as best practices. Although procedures are not yet documented, the Privacy Team is aware of and is current in its review obligations. Of the 23 SORNs and PIAs in place during the time of this audit, the Privacy Team has republished three and notes that the vast majority of the remainder are less than one year old and, therefore, will not come up for review until 2013 and 2014. The policies documenting such reviews will be included in the Bureau's guidance on SORNs and PIAs. The Privacy Team will formalize these policies and procedures as the Bureau matures.

**2012.CR.1 Respond to written inquiry to contact center SLAs. (Risk of Deficiency or Noncompliance).** Consumer Response's outsourced contact center provider (Vangent) receives and processes all consumer written inquiries and faxes, along with most inquiries or complaints registered via phone or the web. For online or phone inquiries, CR has documented clear service level agreements (SLAs) by which Vangent is or will soon be held accountable for performance across most of its intake operations. However, no formal SLA exists for response to written inquiries. Without a comprehensive set of SLAs that tie to the entirety of contact center activity, the Bureau can ultimately hamper its ability to comply with Section 1034(a) of the Dodd-Frank Act, which requires the CFPB to establish "reasonable procedures to provide a timely response to consumers." Therefore, we recommend that Consumer Response add response to written inquiry expectations to formal contact center SLAs.

**Agency Response:** The Bureau concurs with this recommendation and notes that Consumer Response, in coordination with its strategic partners, is currently in the process of evaluating and enhancing all service level agreements with the outsourced contact center provider to include written inquiries from consumers. This task is part of a larger effort to assess and improve CFPB's ability to oversee and refine the quality of the entire outsourced contact center.

**2012.IT.3 COOP Development (Risk of Deficiency or Noncompliance).** Government-wide requirements related to Continuity of Operation Plan (COOP) development, operation and testing are principally outlined within: (i) Title III of the E-Government Act—entitled the Federal Information Security Management Act of 2002 (FISMA)—and accompanying standards promulgated by the National Institute of Standards and Technology (NIST), including Federal Information Processing Standards (FIPS) 199, FIPS 200, and NIST Special Publication (SP) 800-53; and (ii) Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and

Requirements” (February 2008) or FCD 1, developed and published by the Department of Homeland Security in coordination with its interagency partners.

In our FY11 Performance Audit, we recommended that CFPB “[d]evelop and test a Continuity of Operations Plan (COOP) that is specific to CFPB, within the Treasury’s larger plan.” While many CFPB systems are managed by the Bureau of Public Debt and the National Finance Center, the agency continues to expand its internally-managed IT infrastructure, in support of key operating units of the agency. Today, there are significant operational systems and a terabyte data mart managed internally by T&I. The ongoing build-out of the CFPB’s internally-managed IT infrastructure expands the agency’s responsibility for COOP planning, coordination and management. CFPB has begun a comprehensive COOP development effort, but planning and documentation are still in the initial stages. Moreover, CFPB has not yet completed an essential assessment and determination of the agency’s pre-defined Recovery Time Objective/Recovery Point Objective (RTO/RPO) for all major system, in accordance with FIPS 199, FIPS 200, and FCD 1. In the event of a significant interruption or disaster, the RTO/RPO objectives would guide critical decisions regarding communications, personnel, facilities, processes, and systems. The RTO/RPO also outlines the foundational assumptions for overall and detailed component-level COOP planning efforts, guiding preventive and responsive resource requirements under multiple disaster scenarios.

As near-term steps within the agency’s multi-year COOP plan development, we recommend the agency:

- 1) Formally assess, document and obtain approval for its business continuity and recovery RTO/RPO requirements for all major aspects of headquarter and regional operations, in accordance with applicable COOP standards;
- 2) Finalize pertinent policies essential for the viability of COOP planning (e.g., Occupant Emergency Plan); and
- 3) Continue to flesh-out the COOP documents and component plans, based on the approved business continuity and recovery RTO/RPO requirements.

**Agency Response:** The Bureau concurs with this recommendation and is in the process of developing a COOP. Since the Bureau began operations, it has utilized the Department of the Treasury, the Bureau of Public Debt, and National Finance Center technology platforms, which already have robust backup and disaster recovery planning to ensure continuity for the Bureau’s critical system operations.

In addition, the Bureau is moving forward with the development of its COOP and, in the meantime, has implemented a number of contingency processes to facilitate continuity of operations in the event of a significant interruption or disaster. As noted in the Summary

of CFPB Actions, the Bureau has policies in place regarding the Telework Program and Alternative Work Schedules, which provide CFPB employees with remote access to Bureau resources. Furthermore, the Bureau's key systems are backed up and are able to be reconstituted in the event of a disaster or significant outage. The Bureau has documented an IT contingency planning strategy prioritizing this reconstitution of its systems.