UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Inspector General

October 17, 2017

MEMORANDUM

TO: Maureen Ohlhausen
Acting Chairman, Federal Trade Commission

FROM: Roslyn A. Mazer
Inspector General

SUBJECT: FY 2017 FTC Management Challenges

The *Reports Consolidation Act of 2000* requires that the Inspector General provide a summary of our perspective on the most serious management and performance challenges facing the agency and a brief assessment of the agency's progress in addressing those challenges. The management challenges in this document are based on work conducted by the Office of Inspector General (OIG) and discussions with senior leaders at the Federal Trade Commission (FTC).

We identify the following as the most significant management challenges facing the FTC:

1. Securing the Agency's Information Systems and Networks from Destruction, Data Loss, or Compromise
2. Accelerating the Maturity of the Agency's Information Technology Governance Process
3. Improving Acquisition Planning and Contract Management

Some of these are enduring challenges requiring leadership's continued attention. Others are a priority at this time in the agency's development, but may become a less pressing priority in the future. The FTC's progress in addressing management challenges one and two slowed in FY 2017. We will address these and related issues in the OIG's upcoming CyberScope reporting and our FY 2017 FISMA evaluation.

The attached document provides the justification for our assessment. We provided a draft of our assessment to management, and its comments are incorporated into the section headings, "Agency Progress in Addressing the Challenge."

We appreciate leadership's ongoing support for the OIG's independent mission, and we will continue to work with you in addressing these and other challenges the FTC faces in achieving its vital mission. As the FTC continues to focus energy and resources on addressing these challenges, it will significantly enhance its performance and success.

Attachment 1

1. Securing the Agency's Information Systems and Networks from Destruction, Data Loss, or Compromise

The information security and privacy environment is fluid and ever-changing, which means that protecting information assets remains an ongoing and complex challenge for the FTC. The volume and scope of information the FTC routinely acquires and must protect is increasing, and threats are becoming more numerous and pervasive. The FTC cannot effectively accomplish its mission if industry and the public lack confidence that the FTC can protect proprietary information, personally-identifiable information, and other sensitive non-public information entrusted to its care.

The FTC OIG assists by assessing FTC information control procedures, including its annual Federal Information Security Modernization Act of 2014 (FISMA) evaluation of FTC information security and privacy programs. These assessments provide management with an independent, high-level determination of the FTC's ability to protect its information assets; securely and cost-effectively acquire, implement, and manage modern technologies; and maintain a skilled workforce versed in technology and the need to protect information assets.

In its FY 2015 and FY 2016 FISMA evaluations, the OIG recognized the FTC improvements taking place and continued to advocate for continuous monitoring and management improvements. The recommended improvements are intended to improve management's security and privacy planning and oversight while reducing costs through an evolving Continuous Monitoring Management and process improvement system.

In FY 2016, the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), and the OIG community, working through the Council of the Inspectors General on Integrity and Efficiency (CIGIE), continued implementation of an information security "maturity model." The maturity model is intended to provide an assessment of the status of an agency's information security program as well as the agency's capability to enhance the resilience and capability of its information security program. The FTC OIG tailored its FISMA evaluation to align with the maturity model approach and to the FTC's mission, organizational culture, size, and technology architecture.

The results of the FY 2016 FISMA evaluation showed that, while the FTC is improving its capabilities to protect its information assets and modernizing its technology, the maturity of its information security program was not advancing. As the OIG's prior assessments concluded, while the FTC responds quickly to mitigate identified specific vulnerabilities and threats and FTC staff recognize and value information security and privacy, its documentation of policies and procedures and monitoring of the information security environment is deficient. Use of the OMB/DHS FISMA criteria highlights these deficiencies because the maturity model emphasizes the need for a formalized program that is consistently monitored and improved.

We also determined in FY 2016 that the FTC Information Technology (IT) and modernization planning and acquisition documents as of September 30, 2016, did not demonstrate the disciplined planning necessary for compliance with Federal Acquisition Regulation principles, or with Office of Management and Budget (OMB) and FTC requirements and guidance for such a complex

activity; nor did the documents demonstrate a risk-based approach where information security, privacy, and performance risks were identified or considered, or where appropriate mitigations were planned. These deficiencies did not adversely affect the FTC's current ability to protect FTC information assets, but are indicative of a security environment with decreasing effectiveness. For example, the OIG's concerns with management's decision to proceed with a multi-year IT modernization plan without having policies and procedures in place for configuration management were realized in August 2017, when the agency experienced an email outage that affected all FTC staff, contractors, and customers using email and mobile email.

The FTC's practice of correcting information security weaknesses after a problem occurs, characteristic of a Level 2 – Defined program, needs to be advanced to higher maturity levels where programed/automated processes and management oversight anticipate issues and take preventive action before FTC operations and missions experience disruption.

The FTC is working to improve its information security processes and planning. Concurrently, the agency must maintain the integrity and availability of its information assets as it continues to modernize its information systems, reorganize its information technology support staff, respond to new security requirements, and continue to provide reliable mission support. Successfully addressing competing requirements for staff and technology resources will require the continued attention of FTC senior and executive management and a focus on building an information security program on defined, repeatable processes. Information security processes must be repeatable, continually monitored and improved if the FTC is to continue to perform its missions while protecting its information assets and controlling costs.

Agency Progress in Addressing the Challenge

As a result of the evolving changes to the cybersecurity landscape, FTC determined to devote additional resources to address its information security program gaps. In 2017, OCIO hired a seasoned federal Chief Information Security Officer to lead the agency's cybersecurity efforts. Recently, OCIO also received approval to recruit additional FTEs, which recruitment effort is currently ongoing. The new FTEs will, among other things, revise policies and procedures to align with the plan to take advantage of federal programs such as Fed RAMP approved cloud services, interagency-shared services, and other initiatives such as the Department of Homeland Security's Continuous Diagnostics and Mitigation program; efforts that will not only allow the agency to provide improved services to agency users but improve the agency's IT security posture as well. In addition, the FTC will focus its initial continuous monitoring efforts on implementing CAP goals and managing IT assets in the following technical areas: hardware and software management, vulnerability management, configuration management, and privileged user management. These are multiyear projects and will be implemented and managed consistent with anticipated, but not yet issued, guidance from OMB.

Finally, while the FTC agrees that revising its configuration management policies and procedures is a priority and integral to the success of its IT modernization efforts, completion of this work would not have prevented the email outage the agency experienced in August, as the OIG suggests. The root cause for the outage as identified in the Exchange Email After Action Report was a defective antivirus update. This sort of change is one that would never be subjected to the

configuration management process as the time required for, and likely benefit obtained from, such a review would be outweighed by the risk of failing to immediately implement any antivirus update.

2. Accelerating the Maturity of the Agency's Information Technology Governance Process

The FTC depends on IT to perform its missions and associated business objectives. In accordance with federal law, the Chief Information Officer (CIO), in coordination with FTC Bureaus and Offices and appropriate governance boards, defines processes and policies to address information resources appropriately.

At the end of FY 2011, the FTC chartered an IT Governance Program with three governance boards to improve the planning, monitoring, and risk mitigation associated with its information systems. Over the past several years, the FTC improved its IT governance procedures to address increasing threats, changes in government-wide policy and guidelines, and constrained budgets. As reported in the OIG independent Federal Information Security Modernization Act of 2014 (FISMA) evaluations for FYs 2012, 2014, and 2015, the FTC improved its governance policies, procedures, and technical guidance and expanded its use of Capital Planning and Investment Control (CPIC) and investment analysis techniques. In FY 2013, the FTC governance maturation slowed because of needed focus on office consolidations and accommodating policy and priority changes resulting from senior and executive management turnover.

Maturation of the FTC governance process improved planning consistency, oversight, and risk-based decision-making. Similarly, the expansion of Governance Board roles increased Board Member participation in linking investments to business needs and analyzing risks and developing mitigation approaches. For example, recognizing the potential enterprise-level impact of minor FTC IT projects, the Governance Board added "risk" as a requirement for Board review, in addition to the Federal Acquisition Regulation (FAR) cost criteria. Thus, under FTC governance procedures, an investment or project with a high security or performance risk that might affect the FTC's reputation is subject to Governance Board oversight, regardless of investment cost.

In FY 2016, the FTC initiated an effort to improve Office of the Chief Information Officer (OCIO) support operations and accelerate the maturation of its IT Governance program. Key elements of this effort were the reorganization of the OCIO to align support components with business needs and the development of a *Strategy and Transition Plan Security and Technology Services* (IT Strategy). The OCIO completed its reorganization in FY 2016 and issued the IT Strategy on September 30, 2016. While the OCIO conducted activities related to the reorganization and IT Strategy in FY 2016 (e.g., revision of policies, procedures, and support systems), management does not anticipate the impact of FTC improvement efforts from the IT Strategy until FY 2017 or later. This determination affected the FY 2016 FISMA evaluation in that the FISMA Maturity levels focus on the current state (in place policies and practices) for Maturity Levels 1 through 3, and the future or target state for Maturity Levels 4 and 5. Consequently, the OIG FY 2016 FISMA evaluation presented a description of the FTC current state information security environment as strong and robust relative to its ability to protect its information assets, with no concerns specific to the FTC privacy program.

In its FY 2016 evaluation, the OIG assessed the FTC IT Strategy and its planned implementation. The evaluation identified weaknesses in the IT Strategy, its proposed implementation, and associated policies and procedures. The OIG concluded that –

> While the FTC made significant efforts to improve its governance practices, modernization planning and acquisition documents provided as of September 30, 2016, did not demonstrate the disciplined planning necessary for compliance with Federal Acquisition Regulation (FAR) principles, Office of Management and Budget (OMB), and FTC requirements and guidance for such a complex activity; nor did the documents demonstrate a risk-based approach where information security, privacy, and performance risks were considered and appropriate mitigations were evaluated and planned.

The OIG identified the FTC IT Strategy (initiated in FY 2016) as a high-risk project, given its mission impact and estimated cost, warranting increased oversight. Accordingly, early in its FY 2017 FISMA evaluation, the OIG collected information allowing assessment of the agency's progress in securely executing its IT Strategy. The OIG's objective was to identify potential concerns or weaknesses and raise them to FTC management for resolution before there is an adverse impact on FTC information assets, mission, or reputation. The OIG determined that the IT Strategy implementation was not proceeding in a manner that reduced performance risks. Further, the FTC's failure to recognize the relevance of legacy policies and procedures to maintaining effective security increases the adverse impact to FTC information assets.

In FY 2016, the OCIO initiated actions to address the challenge of Accelerating the Maturation of the FTC IT Governance process. Unfortunately, while these actions contributed to mitigating some specific areas of concern, they did not advance the IT Governance process. Part of the problem is timing: the OCIO issued the IT Strategy on September 30, 2016 -- the very end of FY 2016. The IT Strategy schedule proposed performance through the entire FY 2016 to FY 2019 timeframe. While FTC performed some IT Strategy-related activities in FY 2016, it delayed some critical activities (e.g., issuance of the supporting contract vehicle). Further, as shown by the OIG evaluation of IT Strategy efforts conducted in FY 2017, the lack of progress appears to be the result of inadequate planning and the solution approaches pursued. For example, the FISMA Maturity Model stresses the use of formalized processes and procedures and documented, risk-based decisions. The IT Strategy assumes that planning artifacts such as an enterprise architecture that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture will be developed as the modernization project progresses. Thus, the FTC is seeking to acquire components for an enterprise architecture that has not been defined.

The following are the OIG assessments of the challenges associated with the FTC's Governance maturation activities identified for FY 2016 performance and their status as of August 31, 2017:

- Updated Governance Charter

  The current Information Technology Governance Program Charter is dated August 20, 2014. The 2014 Charter focused on the processes and Boards specific to the evaluation and assessment of the FTC information technology environment. The FTC has drafted a policy, identified as the replacement for the 2014 Charter, titled *Information Technology*

Governance Administration Policy (IT Governance Administration Policy or *Policy)*, that is scheduled for completion in September 2017. Our review of the OCIO draft *Policy* shows that OCIO wrote it from a responsibility and authority perspective, as opposed to the procedural focus of the 2014 Charter. Further, the *IT Governance Administration Policy* identifies a number of policy management authorities and advisory councils without describing their relationship to the existing Governance Board structure. Thus, the draft policy does not provide for continuity of in-process Governance Board activities, increasing the performance risk to IT investments.

- TechStats

  As defined in OMB Circular A-130, a "TechStat" is a face-to-face, evidence-based accountability review of an IT investment that enables the Federal Government to intervene to turn around, halt, or terminate IT projects that are failing or are not producing results for the American people." The FTC is now successfully using TechStats to evaluate problem areas, but its efforts have largely focused on specific system-level problems (e.g., mobile phones or issues with legal discovery products) as opposed to the Governance Process. Thus, while the FTC's use of the TechStat process is a valuable tool, it has not had a significant impact on maturing the Governance Process. The FTC could use the TechStat process to analyze the governance process itself and the investments monitored by the Governance Boards. For example, the IT Strategy, the FTC Enterprise Architecture, and the FTC contingency planning program are all appropriate candidates for TechStat reviews because they could provide the analysis necessary to ensure that the FTC is maximizing the use of its IT investments.

- IT Strategy and Transition Plan (IT Strategy)

  The OCIO characterizes the FTC IT Strategy and Transition Plan as a significant contributor to the maturation of FTC IT Governance. The Risk and Policy Management Team described in the IT Strategy conducts continuous review and analysis of business practices, with the goal of improving decision making. The Risk and Policy Management Team is also responsible for governance processes and procedures and for ensuring that IT decisions are made in partnership with business stakeholders. The anticipated results are "increased transparency agency-wide of performance gains, challenges, and actions underway to correct deficiencies," and assurance that policies and procedures are assessed for effectiveness and impact on the budget, performance, and operations services.

  The OCIO planned for the multi-year IT Strategy to result in significant improvements in FTC IT Governance. However, in FY 2017, the IT Strategy had little positive impact on the maturation of IT Governance. A cornerstone of the IT Strategy is the use of blanket purchase agreements (BPA), under which the FTC will acquire cloud resources and related services. The IT Strategy called for award of the BPAs for the fourth quarter of FY 2016; however, the BPA award will not effectively occur before the first quarter of FY 2018, making it already significantly behind schedule. Further, the FTC deferred development of an Enterprise Architecture (EA) until after the BPA award. Thus, the FTC does not have a primary information tool that could be used to help identify IT Strategy components that could

be separately acquired or developed. Further, as described in OMB Circular A-130, the EA should align business and technology resources to achieve strategic outcomes. The process of describing the current and future state of the agency and laying out a plan for transitioning from the current state to the desired future state helps agencies eliminate waste and duplication; increase shared services; close performance gaps; and promote engagement among Government, industry, and citizens. The lack of an EA "that describes the baseline architecture, target architecture, and a transition plan to get to the target architecture" presents a substantial performance risk to successful completion of the FTC IT Strategy. This remains a major management challenge for the FTC.

In FY 2017, the FTC identified risks associated with its legacy IT. The FTC complicated its governance maturity efforts by stating that it accepts the risk with its aging legacy IT in order to focus on migration to cloud services. Implicit in this statement is also the acceptance that FTC may increasingly experience disruptions that compromise the capability to perform its missions and protect its information assets. A general acceptance of risk, while allowable, shows that FTC has changed its focus from maintaining a reliable, secure environment to introducing modernized services with a currently unknown structure, risk, and implementation timeframe. The FTC must recognize that it needs *concurrently* to manage risk to its legacy systems and their information assets while modernizing its IT. This recognition must be reflected in a mature governance structure that fully supports both requirements – stable, secure in place Operations and Maintenance and successful planning and implementation of stable, secure modernized systems.

Agency Progress in Addressing the Challenge

The FTC took several steps toward maturing the agency's IT governance, acquisitions and strategic planning processes during fiscal year 2017.

IT Governance

OCIO took numerous steps to mature and broaden its IT governance structure and operations – all to ensure that the Federal Trade Commission's IT risk management activities support a management framework of organization, mission processes, and information systems consistent with guidance in NIST Special Publication 800-39, Managing Information Security Risk, Specifically, the revised structure was created to better ensure: 1) organization-wide risk awareness and management; 2) continuous improvement via stakeholder feedback; and 3) traceability and transparency of risk-based decisions.

The first major step in this process was the Chairman's designation of the CIO as the senior risk official for Information Technology. Next, the CIO designated four OCIO managers as Policy Management Authorities (PMA) to manage day to day risk and implement the requirements of OMB Circular A-130, Managing Information as a Strategic Resource, including managing risks, artifacts, policies, and procedures in assigned areas of policy authority. OCIO also solicited agency-wide participation on various Advisory Councils, whose members act as subject matter experts (SME) to advise the PMAs, the CIO, and Senior Agency Officials in the program areas outlined in OMB Circular A-130.

The PMAs and the Advisory Councils constitute Tier 2 of a three-tiered, escalating IT risk management structure that provides oversight required to identify, analyze, prioritize, mitigate, and manage risks and issues regarding information systems, mission processes, and the organization at each respective decision making tier – all with the overall objective of continuous improvement. For example, when system owners and authorizing officials (Tier 3) are unable to resolve information systems risks and issues, or issues are determined to affect business processes, the risk or issue is escalated to the PMAs (Tier 2) and the appropriate IT Advisory Council to apply resources and decision-making strategies. Similarly, if the risk or issue cannot be prioritized or mitigated by the Tier 2 PMA governance bodies, or the criticality of risk is such that it affects the organization and requires decision-making or resources not available to the PMAs, the risk or issue is escalated to Tier 1 and the Senior Agency Officials who sit on the Enterprise Risk Management governing body, the Senior Management Council (SMC) for analysis and decision-making. The SMC may choose to accept, mitigate, or transfer the risk or modify the IRM Strategic Plan to manage the risk.

Finally, an IT risk register was established to ensure that the PMAs and the IT Advisory Councils have insight into project risk and issues. The PMAs conduct weekly risk reviews and make decisions regarding risk mitigation. Risks are escalated to the agency's SMC senior risk management officials based on the severity, likelihood and impact. These escalated risks are presented as part of the SMC meetings, which focus on, not only IT risks, but also overall agency risks. Depending upon changes in the risk landscape, the IRM, the agency risk profile, or strategic initiatives may require adjustment. The SMC, the CIO, and PMAs will communicate changes in the IRM and agency risk profile to stakeholders, Advisory Council members, and system owners to guide their IT risk management activities.

The new governance structure is intended to streamline decision making, and broadened the IT governance scope beyond development, modernization and enhancement (DME) investments. It is also intended to ensure that IT, which is integral to the work of the agency, and the risks it poses to organization or mission are properly considered as part of Enterprise Risk Management for the agency. The new structure provides transparency throughout the agency regarding IT operations, maintenance, security, staffing, and budgeting, which directly influences the success of DME projects.

Because the voting members of the SMC, the agency's senior risk review board, is made up of those who served as members of the prior IT Governance Board (i.e., the CIO, Deputy Directors of the Bureau of Economics (BE), the Bureau of Competition (BC) and the Bureau of Consumer Protection (BCP); the Chief Privacy Officer, the Chief of Staff, the Executive Director) there were no specific transition efforts that had to be undertaken to move the Governance Board's functions/responsibilities and on-going projects to the broader SMC board that has responsibility for Enterprise Risk Management for the agency. Although these IT governance process improvements were not formally presented as a "TechStat," (although OCIO has no objection to conducting such sessions for non-investment changes or issues going forward) these changes were presented to, and/or vetted extensively before implementation with, stakeholders throughout the agency. The CIO met with and discussed these proposed changes with the Chairman, the IT Governance Board members, the SAT, appointed representatives to the newly formed IT Advisory Councils, members of the FTC community who attended in In the Know With CIO forums, and others who provide input regarding the business risk associated with IT policy revisions and operational and functional changes. Finally, OCIO drafted a policy revision

to the Administrative Manual reflecting these changes in IT governance, which is undergoing final review before publication.

Strategic Planning/Enterprise Architecture

The IRM Strategic Plan, which is targeted for completion in in Q1 FY2018, will supersede the current IT Strategy and Transition Plan. The finalization of the agency's IRM Strategy is a continuation of the current IT Strategy, building on progress already made, and will support further improvement in the areas of IT governance and planning. The plan will establish a five-year strategy for modernizing the agency's information technology portfolio, proposing a target architecture with a focus on high availability cloud environments, increased mobility, and greater emphasis on mission IT needs. In order to capture a cohesive agency view, in development of the plan, OCIO has met with Offices and Bureaus across the agency to document their needs. Again, while a TechStat was not held on the IRM, the draft IRM Strategic Plan was briefed to the responsible PMA/Advisory Council, which recommended it approval by the SMC, which approval is pending.

The FTC approach to strategic planning is to focus on the performance outcomes. As a result, FTC is using the IRM to drive the decision making on the target Enterprise Architecture and vehicles for IT acquisitions. This approach resulted in progress against the current IT Strategy as demonstrated by the completion of multi-factor authentication through use of Personal Identity Verification (PIV) for access to the FTC network. Progress in this area will continue with multi-factor authentication for regional office staff in FY 2018.

Implementation of the IT Strategy requires improvements to the FTC communications infrastructure. To begin the process, FTC completed a Network Modernization Business Case Analysis (BCA) in FY 2017. The Network Modernization BCA anticipated the user demands of a cloud-based solution set as discussed in the IT Strategy, and resulted in a recommendation for upcoming FTC network modernization. In FY 2017, the FTC began the development of an Enterprise Architecture (EA) program that aligns with the Federal Enterprise Architecture framework. Artifacts for the EA program are currently under development and will align IT systems and applications with agency strategic and performance goals, define the current and target state for the agency's IT footprint, and provide a roadmap for future development and modernization. These documents will establish the baseline as-is architecture. Efforts so far have focused on areas of greatest mission risk and thus have concerned documenting litigation processes through meetings with senior leadership in BC, BCP, BE, and the Office of the General Counsel. In FY 2018, the FTC plans to complete the first round of EA artifacts, further define EA governance processes, integrating security and privacy into the overall EA program.

Acquisitions

The planning for, drafting, and issuance of the BPA was the result of intensive, collaborative work by OCIO and the Acquisitions Division, with the support of an outside contractor. It involved, among other things, significant requirements gathering and market research. The award of the BPA has been delayed, in part, due to the large number of proposals received. This is a good problem to have, as this means industry is interested in partnering in the FTC modernization effort. Moreover, this should translate into competitive pricing and a variety of viable approaches for modernization. The IG's assertions notwithstanding, the agency has not

failed to take action to manage risk, while it has accepted the risk pending implementation of its modernization plan. In parallel with its work on issuing and awarding the BPA, OCIO, and more broadly the agency as a whole, has been reviewing, documenting, and mitigating risks including those IT risks that have the potential for impact on mission services. In addition to the weekly review of risk registers described above, OCIO is actively cataloging end of life hardware and software, and has established Integrated Project Teams (IPTs) to conduct risk assessments on the current state. The IPTs will review and assess the upgrade of end of life software and hardware and, based on mission impact and criticality, and will develop project plans to mitigate risk that will be integrated in the IRM Strategic Plan monitoring effort.

3. Improving Acquisition Planning and Contract Management

The FTC depends on contractor support to meet its mission needs. In FY 2015, the FTC obligated about 20 percent of its budget (approximately $60 million) for contracts for goods and services. In FY 2016, the FTC obligated about 23 percent of its budget (approximately $70 million) for contracts for goods and services, and 16 percent of its budget (approximately $50 million) for non-FTE related IT resources. The FTC's dependence on contractor support will continue to grow, as will the percentage of IT resources, as FTC mission requirements expand with an anticipated increase in economic activity.

Given the current economic and budgetary environment, the FTC cannot expect substantial increases in funding. It must, therefore, ensure the effective acquisition of quality goods and services that meet its needs. Implicit in accomplishing this objective is having consistent, flexible acquisition practices that ensure that goods and services are available when needed.

As recognized by the FAR, effective acquisition and management of goods and services requires a team approach between the customer with the acquisition requirements – e.g., the FTC's Bureaus and Offices -- and the organizational component responsible for conducting acquisitions and managing contracts -- the Financial Management Office (FMO). In addition, within the Federal Government, the agency CIO is responsible for ensuring the effective specification and management of information resources.

For more than five years, the OIG has identified deficiencies in IT acquisition planning, project management, and contract management. The acquisition planning weaknesses resulted in: 1) poorly-defined contract functional requirements, the lack of enterprise level planning that resulted in acquisition of products not appropriately integrating with existing IT capabilities, and the lack of metrics with a user or functional focus that could demonstrate whether delivered IT resources met contract requirements and user needs; 2) contracts that did not include the requirements and metrics necessary to identify poor performance or the tools needed to correct performance issues; and 3) Contracting Officer's Representatives (COR) without the training and resources necessary to identify and properly document and resolve poor performance issues.

In FY 2016, the FTC initiated actions to improve the FMO acquisition and contract management processes and the OCIO IT Acquisition Planning, Project Management, and Contract Management processes. Many of these planned actions have not been in place for a long enough period to allow the OIG to fully assess their impact. The summaries below provide the OIG's assessment of the challenges associated with these initiatives as of August 31, 2017.

FMO Acquisition and Contract Management

COR Education

In FY 2016, the FMO agreed to host quarterly COR training. However, the FMO Acquisitions Division subsequently determined that quarterly training was not adequate and thereafter instituted bi-monthly COR training in February 2016 and expanded training to include maturation of the FTC COR knowledge base, as well as to address current, specific needs. The Acquisitions Division also posted a variety of COR resources online, including sample documents and Procurement Action Lead Time (PALT) requirements for common acquisitions.[1] The use of PALT guidelines should result in more realistic planned acquisition schedules for customers to follow and lower schedule risks.

This FMO initiative should have a positive impact on FTC acquisition processing and contract management. The FTC's Blanket Purchase Agreement (BPA) acquisition for Information Technology Services and Support (ITSS) is a critical element in the OCIO IT modernization initiative, approved in September 2016. The IT Strategy issued at that time assumed that ITSS Task Order awards would commence in the fourth quarter of 2016, and the ITSS Acquisition Plan issued in February of 2017 stated that any "potential delay will impact the FTC's ability to award task orders which are planned to be competed and awarded under the BPA in FY2017." However, the FTC does not expect to award the ITSS BPA until FY 2018 – a full year beyond the initial estimate. Had those involved in planning the ITSS acquisition used the PALT and other COR resources, the risk of schedule delay could have been reduced.

Improved Customer Communications

The FMO Acquisitions Division proposed to improve agency acquisitions by improving customer communications. For example, the Division is scheduling targeted customer meetings and providing liaison support for select customers among the Bureaus and Offices. The FAR recognizes the importance of participants in the acquisition process working together as a team.[2] "The Acquisition Team consists of all participants in Government acquisition including not only representatives of the technical, supply, and procurement communities but also the customers they serve, and the contractors who provide the products and services." [3]

The OIG could not fully assess the impact of the proposed Acquisitions Division changes in FY 2017 because these changes will not generate measurable results until FY 2018 and beyond.

[1] PALT is the approximate number of calendar days from the time the contracting officer accepts a complete acquisition package to the time of award. Agencies establish PALT guideless, based on acquisition size and complexity that define the categories of acquisitions to which the guidelines apply. PALT guidance also generally specifies what constitutes a complete acquisition package.
[2] FAR § 1.102(a)(a). The vision for the Federal Acquisition System is to deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling public policy objectives. Participants in the acquisition process should work together as a team and should be empowered to make decisions within their area of responsibility.
[3] FAR § 1.102(c).

Revised Policies and Procedures

The OIG welcomes the Acquisitions Division's continuous review of all FTC policies and procedures to ensure consistency with federal regulations and strive for improved acquisitions and contractor management.

IT Acquisition Planning, Project Management, and Contract Management

The OCIO reported taking significant steps to improve its IT acquisition processes. The OIG has not had sufficient time to assess the full impact of those actions because most are long-term activities that management only began to implement during FY 2016. For example, the CIO established a new Vendor and Program Management (VPM) division in March 2016, and significant VPM initiatives were not scheduled to start until FY 2017. Thus, VPM has not yet had the opportunity to work with the OCIO customer base and the FMO to establish the working relationships, policies, strategies, and practices necessary to improve the FTC acquisition planning, project management, and governance.

Continued Progress

In the last year, the FTC has demonstrated its commitment to improve acquisition planning and contract management by making changes in many contract acquisition and management areas. Yet, acquisition planning and contract management remains a continuing challenge, particularly in regard to improving the management of information technology acquisitions and operations, which the Government Accountability Office (GAO) includes as a high risk area in its 2017 high-risk report.[4] We will continue monitoring the agency's progress to determine the extent to which the FTC has established an effective framework of controls to guide its acquisitions, its COR cadre, and its contract management process.

Agency Progress in Addressing the Challenge

COR Education

COR education continues to be a priority for FMO management and the Senior Procurement Executive (SPE). In FY 2017, FMO's Acquisitions has continued to hold bi-monthly COR training sessions as begun in FY 2016. Topics in FY 2017 have included overall COR roles and responsibilities, expert witness contracts, the Privacy Office's Privacy Threshold Analysis, unauthorized commitments and the ratification process, COR invoice process training, and an end-of-fiscal-year COR review session. To complement its in person training, the Acquisitions Division offers a wide variety of COR resources online for easy access, including templates, sample documents, and PALT requirements for the most common acquisitions, including new task orders, open market contracts, sole source contracts, and supplies/services contracts through GSA.

[4] GAO 17-317, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, February 2017, Improving the Management of IT Acquisitions and Operations.*

Improved Customer Communications

The Acquisitions Division is working to improve the quality of agency acquisitions by continuing to improve customer communications via targeted customer meetings and by obtaining new staff to serve as acquisition support liaisons for the customers. The SPE customer meetings, initiated in FY 2015, ensure standard topics are discussed, and new requirements are being addressed in an agreed-upon priority order. The Acquisitions Division also helped ensure timely completion of actions by sending reminders in advance of key dates. These improvements strengthened the acquisitions process overall and ensured that all acquisitions were completed timely at year-end.

Additionally, in FY 2017, the Acquisitions Division contracted for three acquisition liaisons, to assist program offices by providing hands on guidance about the acquisition process; assisting customers with initiating contract actions; ensuring the adequacy of acquisition packages; and ensuring that both the Acquisitions Division and the customer maintain transparency and confidence throughout the entire process. In this first year, the liaisons have assisted with over 75 contracting actions for the offices within the Office of the Executive Director, as well as BC and BCP. As a result of their work, the Acquisitions Division has begun to see improvement in the quality in acquisition packages, most notably in requirements definition. Customer feedback for the liaisons has been universally positive, and the Acquisitions Division will continue offering liaison services into FY 2018.

Revised Policies and Procedures

The SPE will continue reviewing all existing policies and procedures to ensure consistency with the latest federal regulations. Additionally, the SPE will continue to identify new policies and procedures that need to be issued. In FY 2017, the Acquisitions Division has published substantial revisions to the FTC's Administrative Manual chapter pertaining to Acquisitions. The updated chapter includes detailed descriptions of FTC's elements of an acquisition package, updated roles and responsibilities, a discussion of government-wide Contracting Officer Representative (COR) training requirements, and a definitions section. The Acquisitions Division has also focused on developing policies specifically for acquisitions staff. In FY 2017, the Acquisitions Division published over 17 such policies, with additional policies planned for FY 2018. Topics of completed policies include market research, documenting small business strategies and awards, closeouts, deobligating unliquidated obligations, and formal acquisition plans, among others. Through this continuous assessment process, the Acquisitions Division will have standardized policies and procedures that will govern contracting actions and provide consistency and efficiency in operation and output of the Acquisitions Division, as well as clear guidance for the program offices. Establishment of policies and procedures is an ongoing effort of continuous review, revision, and tested compliance, as the FAR and industry standards are constantly changing.

IT Acquisition Planning, Project Management, and Contract Management

In FY 2017, OCIO's Strategy and Planning Division (SP) established an approach for managing modernization initiatives in an integrated manner. In FY 2018, OCIO plans to extend project

management practices to non-standard change efforts associated with IT Operations and Maintenance to enable integrated visibility, resource allocation, and priority setting across divisions and support vendors to improve IT capability, customer service, and vendor performance accountability.

Also, OCIO's Vendor and Program Management Division (VPM) continues to work with the FMO Acquisition Division to award the IT Support Services BPA, the strategic contracting vehicle for modernization and sustainment of IT services. The two offices will continue to work closely together to plan and execute the transition of legacy services contracts into task orders under the BPA. The planning and execution for task order transition will follow PALT guidelines and leverage other COR resources developed to reduce schedule delays in the acquisition cycle. The BPA will streamline the IT procurement process and enable the FTC to work with vendor partners to acquire and modernize IT services efficiently and effectively.

In FY 2017, the VPM has taken a few important initial steps to improve the efficiency of the requisition and procurement process by collaborating closely with other OCIO Offices and the Acquisition Office. VPM has taken the central acquisition oversight role by reviewing and approving OCIO acquisitions. VPM has developed a single information source that tracks the acquisition status of all OCIO acquisition and works with Acquisition Office to share and validate information between the two offices. VPM also serves as liaison and the focal point to enhance the efficiency of communication between the two offices. The VPM also developed an IT Acquisition Management Guide in September 2017. The guide includes procedures for acquisition planning and contract administration for IT contracts. The guide defines process and methods for enterprise level IT acquisition planning to ensure alignment with IT strategies and impact to existing IT capabilities are considered in an integrated manner. The guide also defines various methods for improving contractual requirements, including performance-based requirements, performance standards and metrics, end-user oriented outcomes and agile incremental system and service delivery. The guide also established management and oversight processes to ensure performance issues are identified, analyzed, and remediated timely and effectively. VPM plans to extend its oversight role to include IT acquisitions from all Bureaus and Offices. OCIO will continue to evolve and mature its project management approach, particularly as it applies to acquisitions.