



Office of Inspector General

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

October 17, 2016

MEMORANDUM

TO: Edith Ramirez
Chairwoman, Federal Trade Commission

FROM: Roslyn A. Mazer
Inspector General

A handwritten signature in black ink, appearing to read "Roslyn A. Mazer", with a long horizontal line extending to the right.

SUBJECT: FY 2016 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 Maturing the Agency's Information Technology Governance Process
3. Improving Acquisition Planning and Contract Management
4. Acquiring Employee Suitability Determinations

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 has made progress in addressing each of these challenges in FY 2016.

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

**Office of Inspector General
Top Management Challenges at the Federal Trade Commission**

October 17, 2016

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

Protecting information assets is an ongoing and complex challenge for the FTC. Information the FTC routinely acquires and must protect is increasing in volume and scope, and threats are becoming more numerous and pervasive. The FTC cannot effectively accomplish its mission if industry and the public do not have 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.

Over the past three years, OIG FISMA evaluations have reached the same conclusions: FTC security and privacy programs are sufficiently comprehensive to protect the confidentiality, integrity, and availability of FTC information assets; the FTC responds quickly to mitigate identified specific vulnerabilities and threats; and FTC staff recognize and value information security and privacy.

The OIG Fiscal Year (FY) 2015 FISMA evaluation used the new Department of Homeland Security (DHS) guidance that provided information security "maturity model" criteria developed by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The CIGIE model assesses agency establishment of security performance metrics and continuous monitoring of those metrics, i.e., an Information System Continuous Monitoring (ISCM) process. Continuous Monitoring Management is a critical FISMA metric because it has the broadest coverage scope and includes the foundation elements of effective information security and privacy control, assessed in three model domains (People, Processes, and Technology) at five maturity levels (1-Ad-hoc, 2-Defined, 3-Consistently Implemented, 4-Managed and Measurable, and 5-Optimized). In the FY 2015 FISMA assessment, the OIG determined that the FTC meets the criteria for Maturity Level 2-Defined. That means that the FTC has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies, but the agency does not consistently apply those policies, procedures, and strategies.

The FTC is in the process of implementing controls that are assessed by the maturity model, such as increasing the level of staff training to improve the consistency and reporting of security and privacy activities, and ensuring controls are documented, measured, and repeatable. The components of the ISCM and the FY 2015 FISMA assessment underscore the need for the FTC to maintain information privacy and security programs that are continuously evolving and maturing to address changes in threats and mission objectives.

The FTC corrects security and privacy weaknesses as staff become aware of problems. This approach is characteristic of Level 2 maturity within the Information Technology (IT) Security Maturity Model, where weakness identification is more likely to result from staff observation than from automated analysis techniques. The FTC is taking action to improve its capabilities to monitor project status as part of its governance procedures. In its FY 2015 FISMA evaluation, the OIG recognized the improvements taking place but continued to advocate for control monitoring and management improvements that increase management's security and privacy oversight while reducing costs through an evolving Continuous Monitoring Management system.

Agency Progress in Addressing the Challenge

The agency's recently finalized IT Strategy and Transition Plan calls for extensive changes to the FTC's IT environment, such as improving IT security through effective and measurable cybersecurity practices. The plan further details the need for more security-driven performance metrics and increased continuous monitoring to align with the key principles of IT security as stated in NIST's Standards for Security Categorization of Federal Information and Information Systems: confidentiality, integrity, and availability. While the IT Strategy and Transition Plan lays out various future targets in IT security and privacy, the FTC's Office of the Chief Information Officer (OCIO) has continued to evolve in the areas of system and network security and availability throughout the past year.

A critical first step in enhancing both the security of FTC systems and the quality of the IT services provided was improving network performance through simplifying configurations to access the infrastructure. For a number of years, the FTC's IT infrastructure has struggled with network latency and inconsistent end-user experience, especially in the FTC's Regional Office locations. An assessment of the FTC's network revealed complex, redundant, and inefficient configurations, many of which caused latency and increased login and authentication times for end-users. A number of these configurations were undocumented and little justification or reasoning existed for the changes. Over the course of fiscal year 2016, OCIO has implemented numerous changes to the FTC network to improve performance, including decommissioning of unused or duplicative systems across the network, standardization of authentication protocols, reprioritization of network traffic, elimination of redundant data encryption, and configuration changes to the agency's network firewall.

As part of the network improvement project, the OCIO began a regular review of system configurations, performance, and event management data. In late 2015, the OCIO instituted weekly operational status meetings to review system performance and configuration data with discussion of deviations and anomalies in system performance and open security vulnerabilities. These discussions led to greater visibility across the OCIO into potential causes of network

performance degradation and the need for automated alerts and improved system monitoring. The OCIO is continuously working to improve its capabilities in automated reporting of system and network performance, using tools such as Solarwinds.

To build on the progress made under the network improvement project, the OCIO is preparing a revamp of its IT Configuration Management program. The final product of this new configuration management program will be documented system baselines and a process for ensuring all changes in configurations are properly reviewed for potential security and performance risks, documenting the decision and the actions taken to implement the changes, and updating documentation to reflect the new system configurations. This change in process will allow the FTC to manage its system configurations more effectively, which in turn will further secure the network, increase efficiency of operations, improve user satisfaction, and provide increased documentation and governance over changes in critical IT systems.

In response to previous FISMA recommendations to improve documentation of security controls and assessments, FTC is streamlining its management of security documentation through the implementation of Department of Justice's Cyber Security Assessment and Management (CSAM) tool. The FTC's investment in CSAM provides a suite of integrated tools that enable effective FISMA compliance through on-demand access to security control and system documentation in a secured shared-service environment. Information System Security Officers (ISSOs) and system owners update their security documentation on a regular basis within the CSAM system, providing a central repository for critical security documentation, such as System Security Plans (SSPs) and Plans of Actions and Milestones (POAMs). The CSAM application was fully implemented in August of 2015. FTC continues to train staff and define FISMA systems and security controls.

In fiscal year 2016, the FTC continued to develop IT governance practices and procedures as it relates to information security and privacy, as recommended in the FY 2014 FISMA evaluation. During fiscal year 2016, the OCIO presented the agency's progress against Cross-Agency Priority (CAP) goals to the IT Business Council and IT Governance Board, providing an overview of the FTC's IT security posture. These materials offer the governance program members insight into the agency's strengths and weaknesses in IT security and furnish information needed to make informed decisions about investments and projects with security and privacy concerns. Additionally, the inclusion of privacy and security risk detail in the submission of IT business cases, beginning in 2015, further integrates security and privacy with the IT Governance Program.

Even though recent FISMA evaluations offer positive feedback on the FTC's ability to defend information and systems against potential threats and vulnerabilities, FTC continues to research and evaluate new ways to strengthen its cybersecurity posture and keep abreast of emerging threats and security challenges. During fiscal year 2016, FTC executed its first phishing simulation exercise, in which FTC employees received a system-generated email requesting personal information or asking users to click a suspicious link. These training exercises reinforce the principles of IT security and privacy that all FTC employees should follow to protect information and IT systems. FTC also continues to improve information security through the implementation of two-factor authentication using the PIV card. Toward the end of fiscal

year 2016, FTC implemented a limited release of PIV authentication to the FTC network, including the mandatory use of two-factor authentication for privileged users, such as system administrators. The FTC aims to expand the use of two-factor authentication to require mandatory PIV card login for all FTC users during fiscal year 2017.

In accordance with guidance from the Office of Management and Budget, key milestones to address this challenge will be published in the FTC's next Annual Performance Plan.

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

In executing its core missions to promote competition and protect consumers, the FTC generates, receives, and stores large volumes of information. For example, the agency obtains a large volume of proprietary information through its law enforcement investigations, and the agency hosts a national repository of consumer complaints. The FTC depends upon the availability, confidentiality, and integrity of its information systems to complete its missions, protect its information assets, and protect the privacy of individuals whose records are in FTC systems.

At the end of FY 2011, the FTC chartered an Information Technology (IT) Governance Program with three governance boards to improve the planning, monitoring, and risk mitigation associated with its information systems. The Governance Program provided a formalized structure for inclusion of FTC Bureaus in IT planning and investment analysis. Although the governance structure was an improvement, its focus was on management of the investment and not on management of risk associated with those investments.

The FTC has 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 FISMA evaluations for FYs 2012, 2014, and FY 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 to provide consistent planning, oversight, and risk-based decision-making of its IT investments. Further, IT Governance Board members are more proactive, raising security and system performance concerns in materials submitted for review and requiring assessments of risk and alternate solutions to technology advances and challenges. For example, in recognition of the enterprise-level impact of even minor FTC IT projects, the Governance Board now identifies reputational risk as a critical potential impact from a system compromise or failure, and investment risk is now a criterion for determining whether an investment or project is subject to Governance Board review and oversight. Moreover, under current FTC governance procedures, an investment or project with a high risk of an adverse impact from a security breach is subject to Governance Board oversight, regardless of cost.

a. Integrating Acquisition Planning and Project Execution in Accordance with the Federal Acquisition Regulation and FTC Policy Requirements

The OIG FY 2015 FISMA review identified opportunities for further maturing IT governance practices:

- The Governance Boards are, as part of their authorized responsibilities, making decisions

that affect the planning and execution of proposed and ongoing investments/projects. The FTC should improve documentation for these decisions so that they clearly communicate (to an individual who was not a participant in Governance Board discussions) the elements of the decision, including its scope, rationale, and associated risk.

- Approved projects/investments may encounter problems during execution that result in unanticipated delays, cost overruns, or performance issues (e.g., the electronic Discovery Support System (eDSS) for litigation support). The FTC Governance Process does not yet have a process for identifying projects that experience difficulties in performance and escalating those problems for higher level management review and resolution. The FTC should establish escalation processes that automatically identify projects that are outside established performance criteria for higher-level management review, such as a TechStat or other less formal problem status assessment.
- FTC IT operations must adhere to a variety of government-wide law, policy, standards, guidelines, and best practices. Direction regarding these various documents may originate from one or multiple entities. For example, FISMA compliance must take into account the FISMA statutory guidance as well as policy and other guidance originating from the OMB, National Institute of Standards and Technology (NIST), DHS, National Archives and Records Administration (NARA), and General Services Administration. A recent example of multiple sources of guidance is the Controlled Unclassified Information (CUI) program, which started eight years ago as an approach to facilitate secure sharing of unclassified terrorist information. However, with the promulgation of a Final Rule in September 2016, the program has evolved into a government-wide effort that will require a substantial resource commitment for FTC compliance, especially in the areas of labeling and marking current and legacy information. The FTC's monitoring of potential CUI requirements was principally focused on the legal aspects of the program originating through NARA and not on the operational impacts identified in NIST guidance, which originated in a dual track that included both NARA and NIST. Thus, the FTC is only now analyzing the operational impact of this new program. To avoid future instances where FTC must make substantive operational changes, the Governance Program should include procedures where pending government-wide changes are provided to the Governance Boards so that the potential operational impact of the change may be identified, discussed, and if necessary, action taken, particularly in the context of major planned acquisitions likely to be affected by new requirements.

Other OIG evaluations demonstrate that the FTC must integrate both the acquisition planning and information technology elements of the Federal Acquisition Regulation (FAR). FAR Part 7 includes a description of the acquisition planning to be used in supporting the acquisition of goods and services. FAR Part 7 also includes references to FAR Part 39, which specifies requirements for acquisition of information and information technology under guidance and authority of the Chief Information Officer.

In several reviews over the past five years, including the annual FISMA evaluations, the OIG identified the failure to follow FAR and OCIO acquisition policy in the course of acquisition planning as a root cause of cost increases and delivery of products and services that failed to

meet FTC business and operational needs. Had the FTC adhered to the FAR and OCIO Acquisition Strategy requirements for an Acquisition Plan, the risk of accepting poor performing products would have been reduced. For example, in its recent evaluation, *Opportunities Exist to Accelerate Maturation of FTC Information Technology Governance Practices*, the OIG provided close analysis of two projects, each with a high impact on the FTC mission and the day-to-day activities of its work force and contractors: its e-Discovery Support System (eDSS), which provides tools and techniques for review of significant amounts of electronic data in support of litigation activities; and its Messaging Infrastructure Project, which was to replace and upgrade the FTC's Blackberry devices with mobile "smart phones."

Our assessment showed that in approving the eDSS project, the FTC elected to eliminate a Return on Investment (ROI) analysis, a discussion of project milestones and performance criteria, a discussion of the impact on operational use where system support is provided from outside the United States, and a discussion of the impact of deferring development of performance criteria until after contract award -- all elements of an Acquisition Plan.

These reviews demonstrate that the FTC should closely adhere to the acquisition planning process called for in the FAR and by the agency's OCIO Acquisition Strategy. A significant first step has been taken as the FTC is now including representatives of the Chief Acquisition Officer in significant acquisition planning efforts. This should be followed by guidance that allows the content of specific acquisition plans to be tailored based on acquisition complexity, size, and risk and where failure to meet either acquisition milestones or performance criteria are elements of a problem escalation process to the Governance Board.

b. Integrating a Tailored Insider Threat Program into Governance Board Processes

The FTC's planned actions to implement the new CUI Rule present an opportunity to extend the FTC's insider threat program to sensitive but unclassified holdings. The FTC has minimal holdings of or access to classified information, but does have substantial volumes of highly sensitive information about individuals, businesses participating in government programs, and individuals and businesses that submit confidential and proprietary information in regulatory filings. These holdings include consumer complaints, judicial filings, discovery databases, competition merger filings, and other administrative and security information. Inadvertent or deliberate disclosure of such information could cause severe damage to consumers, litigants, regulatory filers, and others.

Previously, FTC protected its sensitive information holdings as "non-public." The non-public designation is now subject to protection under the CUI program that includes general control requirements for information identification and safeguarding as well as protection under specific statutes.

The FTC is considering opportunities to establish an insider threat program that addresses all of its information holdings. Extending its insider threat program to all sensitive holdings follows guidance from NARA and NIST to establish and maintain consistent, risk-based information protection programs across an agency.

Management's planned focus on insider threats is well placed and should be a high priority. To effectively safeguard CUI from insider threats, the FTC should consider expanding its insider threat program to the full scope and range of the FTC enterprise. An enterprise risk focus is consistent with the NIST principles of enterprise risk management and guidance espoused in the Office of Management and Budget's (OMB) recent revision of OMB Circular A-123, *Management's Role in Enterprise Risk Management and Internal Control* (July 2016). Such an effort would also complement recommendations in the OIG's FY 2012 and 2013 FISMA evaluations that urged use of a governance-based capability (such as an analytical software tool) to permit analysis of incident/trouble reports. A governance-based approach to build a tailored insider threat program could meaningfully add to the FTC's information security and privacy protections, as well as risk mitigation.

The FTC is accelerating its introduction of new technologies and use of existing technologies in new ways to keep pace with increasing demands for technological support to satisfy mission objectives; comply with changes in government-wide policy; and increase support reliability while constraining costs. The FTC will need to continue to mature its governance practices to ensure IT projects/investments have a high probability for successful performance with minimum risk.

Agency Progress in Addressing the Challenge

OCIO, in conjunction with agency leadership, took steps toward maturing the agency's IT governance process during fiscal year 2016. In November 2015, the Chief Information Officer (CIO) established a Risk and Policy Management division within the OCIO to focus on the areas of risk management, policy and procedure, and governance. Since the inception of this organization, the OCIO has made great strides in advancing the agency's IT governance program and increasing the visibility of risks and issues associated with the agency's IT programs and systems.

The first major accomplishment was the development of an updated governance program charter. In the updated charter, the roles and responsibilities of the governing bodies, the Information Technology Council (ITC), IT Business Council (ITBC), and IT Governance Board (ITGB), were better defined. Additionally, the new charter improves the governance process through the integration of risk management principles. Incorporating risk management into the governance process ensures the members of the governing bodies are able to make well-informed decisions, considering all risks, including security, privacy, technology, procurement, and human capital risks. The OCIO is working to finalize the charter and ensure alignment with best practices in IT governance, risk management, and capital planning and investment control, with a target completion date of March 2017.

To ensure the governing bodies have insight into project risk and issues, the OCIO expanded the use of the TechStat process. Before the end of FY 2016, OCIO presented TechStats to the governance boards on numerous mission-critical IT investments, including network modernization, disaster recovery, remote access, e-discovery, and the mobile device program. Through the TechStat process, the governing bodies are able to have visibility into variances in cost and schedule, technical challenges, and project risk.

The finalization of the agency's IT Strategy and Transition Plan will support further improvement in the areas of IT governance and planning. The Plan establishes a two-year roadmap 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. This roadmap is broken into a detailed list of projects and initiatives needed to meet the objectives set forth in the plan and acts as a definitive list of potential IT investments for the next two to three years. Both the IT Business Council and IT Governance Board have reviewed and provided feedback on the Strategy and Transition Plan and are in full support of the initiatives and projects proposed. The OCIO is currently reviewing all active projects and potential investments to ensure those projects align with the Strategy and Transition Plan, and those projects that do not align will be reevaluated, de-scoped, or terminated.

The OCIO continues to make improvements to the governance process in preparation for fiscal year 2017. In the future, OCIO will continue to review the IT governance process and recommend changes to better align the process with the budget cycle, integrate privacy and security, and provide increased control and oversight over investments regardless of cost, as well as operational spending, acquisition planning, and enterprise-wide portfolio analysis. The OCIO is in the initial stages of developing a portfolio management program, beginning with the development of high-level IT portfolios (service domains) and programs (service categories) and the assignment of Service Category Managers to each of those areas. The Service Category Manager (SCM) will be responsible for the successful execution of projects and initiatives within the service category and will have greater autonomy over the alignment of resources to individual services and projects. Starting in FY 2017, the OCIO will align both budgetary resources and FTE resources to the service categories established to inform decision-making at a higher, more holistic level, instead of focusing on individual investments. Each service category will have its own program-level plan that aligns with the IT Strategy and Transition Plan to ensure sufficient acquisition planning, requirements analysis, and risk assessment takes place.

Additionally, OCIO is working to build performance metrics associated with each service area so OCIO leadership and governance board members can make informed decisions about investments needed to improve performance and customer success. Another initiative underway in the OCIO is the development of a new program and project management structure. The newly established Vendor and Program Management division is leading the effort to strengthen program and project management through increased documentation, data-driven project decision-making, greater project oversight from the OCIO leadership, and alignment with the IT Strategic and Transition Plan. To address the integration of acquisition planning with the governance process, FTC will update the IT business case analysis (BCA) template to include acquisition-planning elements as described in the Federal Acquisition Regulation (FAR).

Insider Threat Program

While the FTC's Insider Threat Program (ITP) focuses on the protection of classified materials, the Commission has long placed great importance on its mandate to protect CUI from insider and other threats and strives to regularly update and adjust its practices to ensure the security of all non-public data in its control. Under the FTC Act, FTC employees who disclose non-public

information, without authorization, are subject to possible criminal prosecution. Moreover, the FTC has adopted an extensive framework of protections for sensitive, but unclassified information held by the agency. This framework includes documented internal policies and procedures concerning safeguarding sensitive personally identifiable information.

As part of this ongoing effort to protect the non-public information in its possession, FTC staff is reviewing the rule just issued by the National Archives and Records Administration regarding the handling of CUI, *see* Final Rule, *Controlled Unclassified Information*, 81 Fed. Reg. 63324 (Sept. 14, 2016). As part of this process, the Commission will entertain the OIG's recommendation to consider expanding the scope of the agency's insider threat program, and how the agency might leverage its insider threat program to protect CUI.

The ITP requires an implementation plan to gather, share, integrate, identify, and report relevant insider threat information from offices across the agency, including security, information security, and human resources. FTC plans to implement the ITP in phases, and will identify staff responsible for planning, implementing, and operating each element. FTC has already established a multi-office working group, chaired by the Records and Filings Office (RFO) and that includes the Chief Privacy Office, the Chief Information Security Officer, representatives from Physical and Personnel Security, the Office of General Counsel and others, to develop plans to implement the requirements of the final CUI rule and consider the implications these changes will have on the ITP.

FTC's Privacy Office will work to ensure a balance between a robust and effective ITP, using NIST's risk management framework analysis, and the privacy rights of FTC employees under the Privacy Act and other federal laws. Staff training is critical and a web page of materials to educate FTC staff about insider threats will be launched on FTC's intranet in December 2016. Also, OCIO is revising the Risk Management and Governance policy to require that systems that may include CUI be identified as such. Additionally, OCIO's FISMA policies will be revised to ensure that the control requirements of the CUI program, as identified in NIST security special publications, are taken into consideration when planning for systems and selecting information safeguard controls. OCIO will review capabilities for CUI marking and metadata analysis, and verify and validate that potential technology acquisitions, when feasible, address these requirements. OCIO currently logs bandwidth utilization and reviews the logs on a monthly basis looking for any anomalous file transfer amounts that might indicate an exfiltration of data out of the Commission. OCIO, in consultation with others, will also review its ITP and data loss prevention capabilities and recommend solutions to enhance our capabilities in both areas. RFO will, among other things, continue to monitor NARA and NIST CUI program activities and alert agency officials of changes that affect the agency's approach to managing CUI on its systems.

In accordance with guidance from the Office of Management and Budget, key milestones to address this challenge will be published in the FTC's next Annual Performance Plan.

3. Improving Acquisition Planning and Contract Management

The FTC continues to rely on contract support to meet its goals and objectives. In FY 2015, the FTC obligated approximately \$60 million – or about 20 percent of its FY 2015 appropriation –

for contracts for goods and services. Effective contract management is essential to ensure that the FTC obtains the quality goods and services it needs with expected quality performance, and that it receives goods and services on schedule and within contracted prices.

For more than five years, the OIG has identified deficiencies in IT acquisition planning, project management, and contract management. For example,

- The FTC Data Center project known as Information Technology Architecture Release 1 (ITA-1) deficiencies resulted in a special OCIO initiative to research and attempt to mitigate the deficiencies and acquire a new infrastructure support contractor;
- Performance and capability issues in the electronic discovery platform (eDSS) obtained to provide litigation support IT capabilities did not provide the anticipated capability, reliability, or scalability needed, resulting in continuation of legacy systems that had been planned for retirement, special efforts to try to diagnose and remedy identified deficiencies, and use of alternative products that could provide needed capabilities; and
- A contract for Targeted Reviews to conduct analyses and develop reports to help the OCIO in their strategic planning efforts that resulted in the generation of unnecessary reports, where the OCIO staff served as contractor resources to develop required reports while maintaining their own workloads.

OIG analyses showed that defective acquisition planning and weaknesses in contract management contributed toward these contract failures. Effective contract management is a function of a properly constructed contract; consistent, product/user focused performance reporting; and a trained Contracting Officer's Representative (COR) with the resources necessary to monitor contractor performance and address poor performance.

In FY 2016 the OIG completed several reviews of the FTC's efforts to address the long-standing challenge to adequately provide qualified COR support. For example, in our evaluation of the OCIO, the OIG identified shortfalls that increase the agency's risk for poorly performing IT contractors and vendors, resulting in undelivered or delayed capabilities and functionality, and performance challenges that jeopardized mission success. A key finding was that the FTC has not been successful in recruiting, training, retaining, and supervising CORs. For example, we found that OCIO employees who serve as CORs may be assigned as many as 15 individual contracts and often lack project and contract management skills; OCIO did not provide guidance to address situations where requirements expanded beyond contract limits ("scope creep"); and The FTC did not provide guidance or support to CORs to enable them to properly manage or modify contracts that did not specify proper performance metrics, and did not define the process for collecting or measuring performance against objectives.

The adverse impacts of IT problem contracts are not consistently reflected in performance metrics. For IT contracts, the FTC typically used metrics that monitor performance (e.g., availability and system down-time) for individual components and not the service levels provided to end-users. Component-focused metrics often result in higher performance levels than experienced by the end-user. This places the CORs in a situation where they cannot effectively

address user performance complaints -- a situation that increases stress on both the COR and the end-user.

CORs with inadequate contract management training and skills also have an increased potential to overlook issues that are critical to proper contract management. For example, the OIG received complaints that some CORs might not be retaining emails in contravention of federal regulations and FTC records management policies; non-COR FTC staff were directing contractor performance; and some CORs may not be properly documenting poor contractor performance, precluding potential remedial contract action. The FTC should staff and train FTC CORs so they can effectively monitor contractor performance and ensure that the FTC receives the quality goods and services they need in accordance with contract costs and schedules. FTC should ensure that contracts include provisions for providing performance metrics that effectively support COR responsibilities, and that COR workloads are adequately balanced so that they have the resources necessary to perform their oversight role.

Agency Progress in Addressing the Challenge

COR Education

COR education continues to be a priority for Financial Management Office (FMO) management and the Chief Acquisitions Officer (CAO). While in FY 2016, FMO agreed to host quarterly COR training, the Acquisitions Division subsequently determined that there was a need for more frequent training and has held bi-monthly COR training since February, 2016. Bi-monthly training will continue and will not only address current, specific COR needs, but also will be tailored towards maturing the FTC COR community's knowledge base overall. To complement its in person training, the Acquisitions Division has posted 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.

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 acquisition liaison support for certain customers. The CAO customer meetings, first initiated in FY 2015, ensure standard topics are discussed, and new requirements are being addressed in an agreed-upon priority order. This process better supports the Acquisitions Division and the program offices to engage in integrated acquisition planning.

Additionally, the Acquisitions Division has contracted for three acquisition liaisons, who will assist assigned program offices, beginning in early FY 2017, by providing hands on guidance on 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 visibility and confidence throughout the entire process. The liaisons also will assess the current state of services received, so that they can structure subsequent acquisitions to continuously improve the quality of contractor services. Liaisons will begin with the end goal in mind, providing acquisition assistance that will ensure the customer based performance management measures are built in to the acquisitions package at the requirements definition

phase. FMO anticipates that the liaison support will improve the quality of the acquisition packages, which will lead to better management of contractor performance, as well as delivery of improved services to the Commission.

Revised Policies and Procedures

The CAO has continued to review of all policies and procedures to ensure consistency with the latest federal regulations. The first phase of this effort included a review and draft revision of the Administrative Manual section pertaining to Acquisition, which was completed in FY 2016. Review and revision of the policy on Market Research and Acquisition Planning will be completed in the second quarter of FY 2017. The Acquisitions Division will continue to identify areas of concern that need established policy and procedures in FY 2017 and beyond. Through this continuous assessment process, the Acquisitions Division will have legally compliant and 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 in the acquisitions environment.

IT Acquisition Planning, Project Management, and Contract Management

OCIO has taken significant steps towards improving IT acquisition processes during FY 2016. In March 2016, the CIO established a Vendor and Program Management (VPM) division within OCIO to focus on IT acquisition, contract management, and program management processes and practices. The VPM division works with IT managers, IT governance stakeholders and the FMO's Acquisitions Division to develop strategies, plans, processes, and procedures for identifying, reviewing and validating IT acquisition requirements; integrate IT acquisition planning with capital planning and project planning; develop acquisition strategies and mechanisms to streamline and reduce the number of individual acquisition actions; establish guidelines and standards for defining measurable and meaningful contract performance metrics; establish procedures and methods for ongoing contract performance monitoring; and provide training and skills development for OCIO staff in acquisition planning, project management and contract management. By the end of FY 2016, OCIO staffed the VPM with three employees with COR and Project Management certification and experience.

The VPM will serve as OCIO's central review and coordination point for all IT acquisitions. It will provide training, coaching and mentoring to CORs and Technical Point of Contacts in other OCIO divisions regarding IT acquisition and IT project management. VPM staff will also serve as CORs on complex IT acquisitions. In FY 2017, OCIO will continue to assess resource requirements of the VPM and take necessary actions. OCIO will also assess and invest in training of all OCIO staff in acquisition and project management areas.

In FY 2016, the VPM has been working in conjunction with FMO's Acquisitions Division to develop a Blanket Purchase Agreement (BPA) strategy to streamline acquisition of IT services and to implement the agency's IT Strategy and Transition Plan. The BPA will provide a mechanism for FTC to acquire strategic partners to support the agency's IT service delivery,

reliable and secure infrastructure operations, and modern and innovative IT solutions. The BPA will establish clearer expectations of services and service integration among contractors, put in place standard methods of procuring needed services, and improve acquisition process efficiencies. In FY 2017, OCIO and FMO will continue to work very closely together to: 1) define requirements and solicitation packages for the BPA and its task orders; 2) transition legacy service contracts to the BPA; and 3) develop a strategy in FY 2017 to streamline and reduce the number of IT commodity product acquisition contracts. OCIO plans to award the BPA by April of 2017.

In FY 2017, OCIO will conduct a comprehensive review of existing IT acquisitions policies and procedures, develop new or updated IT acquisition policies and procedures, and ensure their compliance with CAO's established agency-wide policies and procedures. OCIO will also establish a mechanism to enforce the procedures. OCIO will ensure that IT acquisition and contract management procedures are integrated with capital planning, program management and IT governance. OCIO will ensure that all key IT acquisition stakeholders will be engaged in the process, including OCIO staff and managers, business customers, and the agency's IT Business Council and Governance Board members. OCIO will focus on COR training, acquisition planning, performance metrics, and ongoing contract performance monitoring for IT acquisitions.

In accordance with guidance from the Office of Management and Budget, key milestones to address this challenge will be published in the FTC's next Annual Performance Plan.

4. Acquiring Employee Suitability Determinations

Protecting employees, contractors, and members of the public who work in or visit FTC facilities requires clear policies, protocols, and effective management oversight. All agency facilities must adhere to specific General Services Administration security standards and Office of Personnel Management (OPM) personnel security practices. In addition to physical threats, the agency must adhere to Federal Information Security Modernization Act of 2014 (FISMA) standards to protect its technological infrastructure from cyber threats and other risks to information security and privacy.

The Administrative Services Office (ASO) is responsible for managing physical security, health, and safety programs for agency staff and facilities, while the Human Capital Management Office is currently responsible for personnel security. There are approximately 1,700 federal employees and contractors that constitute the FTC workforce and require a secure working environment. In addition to visitors, there is a steady flow of arriving and departing staff who must be "onboarded" – that is, processed into the agency.

The agency must adhere to the appropriate security regulations for onboarding. In accordance with Executive Order 10450, *Security Requirements for Government Employment*, and Title 5, Code of Federal Regulations (CFR), parts 731 and 736, the FTC requires personnel security investigations to determine if applicants, interns, volunteers, contractors, and employees meet the suitability requirements for employment, and for physical and logical access to its information and IT systems. Although OPM requires a suitability determination for all potential employees,

there is no mandated process for onboarding new hires, which is left to the discretion of the individual agency.

OIG and Government Accountability Office reporting throughout the federal government demonstrate that onboarding employees prior to suitability determinations is an agency security threat. An OIG FISMA review found in 2013 that the FTC had provided credentials to access the agency's IT infrastructure prior to completion of minimum background screening, contrary to FTC policy, making the agency vulnerable to insider threats. The OIG recommended in its FY 2013 FISMA evaluation that the FTC revise its infrastructure access procedure to enforce the access restriction until the completion of background screening. The 2013 recommendation remains open today and was restated in the OIG's FY 2014 and FY 2015 FISMA reviews.

In response to the OIG's FISMA recommendations, the agency has committed to align infrastructure access procedures with FTC access policy. ASO (which at the time was responsible for personnel security) adopted an informal pilot program in the summer of 2015 granting contractors physical access to FTC buildings upon onboarding through the issuance of a temporary badge allowing physical access to FTC facilities, but withholding network access until the contractors are fingerprinted and receive favorable determinations from ASO. FTC policy currently requires all new employees and contractors to have their fingerprints adjudicated prior to allowing network access. When fully implemented, this change may resolve a key finding in the OIG's 2015 *Evaluation of the Office of Chief Information Officer*, which noted that Bureaus have effectively bypassed FTC policy governing IT requests by pressing for premature onboarding of staff. The agency can no longer defer implementing the OIG's 2013 onboarding recommendations and must urgently address internal control improvements identified in recent OIG referrals and in management's parallel review of recently discovered lapses in physical and logical accesses associated with its special hiring and other programs. By addressing gaps in policies and operational oversight through sustained leadership focus, the FTC can more effectively protect its staff, contractors, and the public, and safeguard its property and repositories of highly sensitive information in support of its competition and consumer protection missions.

Agency Progress in Addressing the Challenge

The Office of Personnel Management (OPM) is directed to provide guidance to civilian agencies on the handling of suitability investigations, reinvestigations, and responses to unfavorable determinations. While reporting obligations and the re-investigative process are both well-defined for individuals with clearances, there is no clear OPM guidance on suitability and fitness or on the handling of the re-investigation of public trust personnel. Despite this lack of guidance and the discretion granted agencies in handling the onboarding of personnel, management agreed with the OIG that there were potential vulnerabilities associated with onboarding employees and contractors before completion of fingerprinting and preliminary suitability/fitness background screening. Accordingly, based on its assessment that the risk was greatest with respect to contractors,¹ in 2015, the agency first implemented a policy requiring that all contractors be

¹ Certain characteristics of the agency's makeup operate to lessen the risk of non-suitability for a significant percentage of the agency's FTE hires. The FTC is largely made up of lawyers who, by virtue of most bar rules, are

fingerprinted and a preliminary suitability/fitness check be completed before granting them logical access.² By the end of December 2016, the agency will have implemented a new process that will ensure that contractors and employees are on boarded and granted logical and physical access, only after they have been fingerprinted and a preliminary suitability/fitness determination has been completed. Employees and contractors also will be required to have successfully completed privacy and security training before being on-boarded.

These changes will be supported by implementation of new electronic systems, including the Workforce Transformation Tracking System (WTTS), which will track the onboarding of FTE, and the Entrance on Duty System (EODS), which will manage relevant documentation related to onboarding. The agency is also modifying its CICOM (Check In Check Out Moves) system to be able to better track and control the onboarding of contractors and all other employees. All system implementations and modifications will be completed by the end of February 2017. All policies and procedures related to these and other changes being implemented to guide hiring officials and protect the agency, with respect to the complete array of its hires, will be in place by the end of March 2017.

In accordance with guidance from the Office of Management and Budget, key milestones to address this challenge will be published in the FTC's next Annual Performance Plan.

subject to ethics checks to be admitted to practice and to ongoing obligations to self-report entry of judgment in certain civil actions, charges by indictment or information, all felony convictions, and certain misdemeanor convictions. The fact that one could lose one's license to practice law for committing or failing to report such acts is strong disincentive not to engage in such behavior. Moreover, once onboard, all FTC employees are subject to Section 10 of the FTC Act, 15 U.S.C. § 50, pursuant to which unauthorized release of information obtained by the Commission is a criminal offense, with penalties up to a \$5,000 fine and one year imprisonment, or both. In some cases, criminal sanctions may also be available under the Trade Secrets Act, 18 U.S.C. § 1905, or the Larceny Act, 18 U.S.C. § 641. Thus, even where employees have been on-boarded before completion of a suitability determination, strong disincentives are in place and continue to serve to protect against misuse of the agency's highly sensitive information.

² Despite certain violations of this policy, for which the employee involved was disciplined, the on boarding of contractors after fingerprinting has been successful.