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

Office of Inspector General

October 15, 2015

MEMORANDUM

TO: Edith Ramirez
Chairwoman, Federal Trade Commission

FROM: Roslyn A. Mazer
Inspector General

SUBJECT: FY 2015 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. Maturing the Agency's Information Technology Governance Process
3. Improving Contract Management
4. Stabilizing the Agency's eDiscovery Support System
5. Ensuring Compliance with Digital Records Management Requirements

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 2015.

The attached document provides the analysis and 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 15, 2015

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 Federal Trade Commission (FTC). The challenge is exacerbated by the increasing volume and scope of information provided to the FTC on both a voluntary and compulsory basis. The FTC cannot effectively complete its missions if it loses the confidence of industry and the public that it can protect the trade secrets and other sensitive non-public information entrusted to its care.

The FTC Office of Inspector General (OIG) assists by assessing FTC information control procedures including conducting the annual Federal Information Security Management Act (FISMA) effectiveness assessment of FTC information security and privacy programs. These assessments provide FTC management with an independent, high-level determination of the FTC's ability to protect its information assets; the capability of the FTC to securely and cost effectively acquire, implement, and manage modern technologies; and maintain the skilled workforce necessary to securely use technology to complete their responsibilities. In the FISMA assessments, the OIG determined that the FTC has robust privacy and information security programs that are in substantial compliance with FISMA and legislative requirements, government-wide policy, and technical guidance. The FTC can adequately protect its information assets and has done so while addressing organizational and technological changes, including modernization of the FTC infrastructure.

However, the OIG Fiscal Year (FY) 2014 FISMA evaluation underscores the need for the FTC to maintain information privacy and security programs that are continuously evolving and maturing. Recognizing the critical need for flexible, robust, and monitored information security control environments, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) revised federal security guidance to allow Departments and Agencies (D/A) to tailor information protection solutions to their organizational needs and missions. While the OMB and NIST guidance now allows D/A greater flexibility, this flexibility comes with a price: D/A managers must establish and maintain clear practices for planning, acquiring, implementing, maintaining, monitoring, and protecting its information technology assets, including hardware, software, and information.

In its FY 2014 FISMA report, the OIG identified the need for improvement in FTC planning and management of its information technologies. As a primary area for improvement, the OIG's FY 2014 FISMA evaluation highlights current deficiencies in FTC risk assessment and management. These techniques are used to identify vulnerabilities and develop the safeguards and countermeasures the FTC needs to deploy to avoid or minimize risk to its systems, operations, and

data. Weak Information Technology (IT) planning and management can result in inaccurate or delayed risk assessments and risk management, which ultimately results in increased potential for loss and mission failure. The evaluation questions if the FTC is equipped to perform risk management that keeps pace with the rate of technological change. The findings focus on enterprise-level issues, recommending that the FTC's Information Technology governance procedures develop into more mature enterprise risk management capabilities, including a clear focus on management of information risk associated with its investments. Developing more mature information processes will ensure that FTC security and privacy programs continue to provide high levels of protection for FTC information assets, but with less workforce stress, greater operational consistency, and improved security.

Agency Progress in Addressing the Challenge

The Office of the Chief Information Officer (OCIO) is working on a number of information technology initiatives that will protect the agency's networks, systems, and data from compromise and loss.

In compliance with FISMA, the OCIO implemented the Cyber Security Assessment and Management (CSAM) tool managed by Department of Justice. CSAM provides OCIO with a mechanism for managing FISMA compliance by: 1) providing centralized and up-to-date information, checklists, analysis, and tracking capabilities; 2) ensuring efficient and effective management of vital resources and data; 3) ensuring best practices and that resources are accessible to assess and manage risks and vulnerabilities across the organization; and 4) supporting Certification and Accreditation (C&A) of FTC's network and mission systems. The CSAM tool allows the OCIO to more readily access information about its systems that will in turn allow for better planning and FISMA compliance across the enterprise. It will also afford the OCIO better visibility into the status of critical security artifacts and documents.

To further improve the agency's risk management posture and ensure FTC systems are secure and protected from external threats, the OCIO, in conjunction with the Chief Privacy Officer (CPO) staff, is working to improve the agency's Information Security Continuous Monitoring (ISCM) program through implementation of a vulnerability risk management (VRM) process. The objective of this initiative is to increase awareness and improve management of internal security risks by formalizing a more streamlined process through which risk can be identified, evaluated, documented, remediated, and easily understood by critical actors throughout the agency. Once fully implemented, this standardized approach to risk management will give all agency senior officials an immediate understanding of the risk posture of the agency. The outputs of the VRM process will be used to fine-tune the agency's Continuous Diagnostics and Mitigation (CDM) process.

Also in FY 2015, the OCIO staff, working in tandem with the Department of Homeland Security (DHS) and in coordination with representatives from throughout the agency, determined which agency systems require increased redundancy and resiliency. Base on this work, a draft business impact assessment has been submitted for management review. As part of this assessment, the OCIO will ensure that any disaster recovery or redundancy solution is secure and protected against

attacks and malicious activities, especially those systems that process or store personally identifiable information (PII) or other sensitive data.

To further improve the agency's ability to manage enterprise risk, the OCIO collaborated with IT Business Council and the IT Governance Board to update the agency's IT governance program, incorporating risk management into the IT investment approval process. The OCIO updated the business case template for proposed IT investments to include a risk analysis and risk mitigation plan. Specifically, proponents of various IT investments are required to detail risks in areas such as cost, schedule, and business impact and provide a mitigation strategy for each risk. They are also required to identify the specific risks associated with privacy and security implicated by the proposed investment, including whether the proposed software or hardware will house PII or poses the potential for a loss of data. The OCIO also updated the IT governance program charter to require IT investment business cases and Board review for investments deemed "high-risk" or "high-impact to business operations," regardless of the cost of the investment.

Other recent OCIO initiatives address security challenges by increasing the security of networks and systems FTC staff use daily to prevent data loss and unauthorized access to sensitive information. For example, the OCIO improved its secondary storage environment to provide additional security for offsite backup storage and reduce the risk of data loss. As part of this initiative, the OCIO transitioned all backup data to a secondary, backup disk storage network, located at the Commission's auxiliary data center. This new backup storage system is less susceptible to failure and provides the Commission with a more secure and more reliable form of backup data storage.

The OCIO is currently working with the Bureau of Economics to implement more robust data monitoring and logging in the Secure Investigative Lab (SIL) environment. The SIL houses some of the Commission's most sensitive data, including PII and Sensitive Health Information (SHI) used in economic analysis in support of investigations and litigation. To detect and reduce the risk of data exfiltration and loss, the OCIO developed a comprehensive logging, auditing, and notification process, which monitors the modification and movement of any data. This process provides the Bureau of Economics and the OCIO with an audit trail for the loss of sensitive data or unauthorized access or modification to PII and SHI.

As part of its enterprise risk management efforts, the OCIO actively evaluates the inventory of IT software and hardware to determine which products are high-risk for the agency. This includes working to replace and upgrade aging infrastructure components and software to decrease the overall number of vulnerabilities in the environment and risk of failure. In FY 2015, OCIO began multiple projects to replace unsupported products, such as the replacement of the network infrastructure at the Commission's Headquarters building, the upgrade of software and operating systems, such as Microsoft SQL Server and BMC Remedy IT Service Management, and the decommission or migration of applications built on unsupported platforms, such as Microsoft Windows Server 2003. Additionally, the OCIO replaced the agency's mobile device management (MDM) software with a new platform that provides continuous monitoring and FISMA 2.0 compliance enforcement, restricts access to authorized agency employees, and enhances security controls for the Commission's mobile devices. Additionally, the new MDM decreases the threat

of compromise or data exfiltration by preventing the installation of unauthorized applications.

In addition to securing individual systems, the OCIO is working to improve the Commission's overall IT security posture enterprise-wide. The OCIO continues to use tools and techniques to monitor events, detect attacks, and provide identification of unauthorized use of the system. These tools and techniques include, but are not limited to, intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, and network monitoring software. The OCIO actively monitors all inbound and outbound communications that occur over networks external to the FTC, including publicly available systems, for unusual or unauthorized activities or conditions (e.g., the presence of malicious code, the unauthorized export of data, or signaling).

The OCIO monitors information systems daily and audits monthly for unauthorized remote connections, and takes the appropriate action if they discover an unauthorized connection. The OCIO uses cryptography to protect the confidentiality and integrity of remote access sessions and routes all remote access through a limited number of managed access control points and protects wireless access via authentication and encryption.

Finally, to continue to improve overall IT security, the OCIO has engaged with the DHS to implement its government-wide Continuous Monitoring Dashboard. The OCIO is also working with the DHS to implement the EINSTEIN 3 (E3A) Program. EINSTEIN 3 is an advanced intrusion prevention system that detects malicious traffic targeting the FTC's networks and prevents that malicious traffic from harming FTC networks. The system provides greater analytical tools and historical data to allow agencies to better analyze trends in vulnerabilities and attacks. Additionally, the system provides enhanced real-time alerts to allow the agency to respond to an event faster and more effectively.

2. Maturing the Agency's Information Technology Governance Process

As evidenced by the number of reports issued by the Government Accountability Office (GAO), OMB, and agency Inspectors General, effective governance of IT investments is a weakness throughout the federal government. The weaknesses are typically in planning and monitoring IT investments as they move from conception through development to operations and maintenance. The weaknesses result in systems/projects that are not delivered when required, often exceed cost projections, and fail to deliver specified reliability, performance, and security. Systems that perform as required, are reliable, and protect information assets are critical to the FTC.

The FTC has a number of responsibilities related to protecting consumers, including advocating for protection of consumer information and consumer privacy. For example, filing with the FTC is a legal requirement for most mergers and acquisitions, and the agency hosts a national repository of consumer complaints. The scope and impact of FTC activities leaves the general public with an outsized perception of the size of Commission. The FTC is dependent on the reliability and integrity of its information systems to complete its missions and protect its information assets. Consequently, the FTC is dependent on the quality of its investment analysis and IT governance

practices to ensure that its workforce has the information management and analysis capabilities it needs.

At the end of FY 2011, the FTC chartered IT governance boards to improve the planning, monitoring, and risk mitigation associated with its information systems. In FY 2012, the agency adopted its new governance structure and improvements commenced. While the governance structure was an improvement, its focus was on the management of the investment and not on management of risk associated with those investments. For example, an investment of less than $500,000 would not be subject to governance board procedure, regardless of the potential loss that the FTC might experience should there be a security breach.

As part of the agency's annual FISMA evaluations, the OIG reviews governance board activities to assess progress toward a mature planning and oversight structure. Our assessments showed that the FTC is continually improving its governance practices. For example, investment risk was elevated as a criterion for determining whether an investment/project is subject to governance board review and oversight. Under current procedures, an investment/project with a high risk of an adverse impact from a security breach is subject to governance board oversight, regardless of cost. Further, the agency now identifies reputational risk as a critical potential impact from system failure.

In our FY 2013 and FY 2014 FISMA reports, the OIG issued recommendations for improving and maturing the FTC governance processes. The FTC and its Office of the Chief Information Officer (OCIO) are addressing all OIG recommendations. The OCIO requires all bureaus and offices to submit business cases for new or significant changes to IT investments for development, modernization, or enhancement whose lifetime cost exceeds a certain threshold, as well as high-impact and high-risk investments. However, documentation still does not consistently capture the rationale behind a decision, anticipated completion impediments and risks, and risk mitigation strategies. Significantly, FTC risk management still focuses on individual investments and not the enterprise analysis contained in NIST guidance; and OMB and the Department of Homeland Security now require an assessment of the maturity of continuous monitoring practices in accordance with the maturity model promulgated by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

In FY 2016, the OIG will complete an assessment of the FTC IT governance structure to determine whether practices have sufficiently matured to effectively address investment and risk management challenges; challenges resulting from a need to provide the FTC workforce with new technologies and techniques that improve their ability to complete their missions while containing costs and protecting FTC information assets; and whether FTC continuous monitoring practices are addressing the CIGIE maturity model.

Agency Progress in Addressing the Challenge

The OCIO, in conjunction with agency leadership, made steps toward maturing the agency's IT governance process during fiscal year 2015. The OCIO collaborated with the chair of the Technology Council (now the IT Business Council) to develop an updated governance program

charter. In the updated charter, the roles and responsibilities of the governing bodies – the IT Council, IT Business Council, and IT Governance Board – were better defined. The criteria for IT investments included in the new charter now require all investments considered "high-risk" and "high-impact" to be reviewed and approved via the IT governance program, regardless of investment amount. The business case analysis template was updated, as well, to better address risk, security, and privacy concerns. The investment business case must now include potential risks and mitigation, security considerations, and whether the investment will involve personally identifiable information (PII) or other sensitive data. Additionally, business cases must receive written concurrence from the Chief Privacy Officer (CPO) and the Chief Information Security Officer (CISO). Once the charter and business case analysis templates were finalized, the new process was used to develop, review, analyze, and approve 16 business cases for IT investments, including investments in business system enhancements, a new acquisition management system, and replacing end-of-life network and server components.

After the FY 2015 investment cycle was completed, the governance program focused on the execution and control of approved investments. A new process was implemented to regularly review the status of current investments at all levels of the governance program. Part of this process included the implementation of Tech Stat briefings to both the Business Council and the Governance Board on large-scale, mission critical IT projects, such as the eDiscovery Support System and the rebuild of SAFE. Through the Tech Stat process, the governing bodies are able to have visibility into variances in cost and schedule, technical challenges, and project risk.

The OCIO continues to make improvements to the governance process in preparation for fiscal year 2016. The OCIO worked with all organizations across the FTC to build a portfolio of potential investments for FY 2016 and issued guidance to the organizations on which investments would require a business case and how to build the business case. 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 and enterprise-wide portfolio analysis. The OCIO is also working with the governance members to build a repeatable and quantitative process for prioritizing and approving investments. This process would assist the governing bodies in determining the relative priority of an investment based on alignment with the FTC's strategic plan, investment criticality, and risk.

3. Improving Contract Management

During FY 2014, the FTC obligated $104.9 million – about one-third of its operating budget – on contracts for goods and services. Contractors assist with the deployment, operation, and maintenance of consumer databases and provide webhosting services. The FTC also has contracts for legal research tools and with software providers. In FY 2014, the highest dollar value contracts were for network infrastructure support ($3.8 million), expert witness services ($2.4 million), and telecommunication services ($2.2 million).

The FTC faces challenges with aspects of its contract management system, particularly with the Acquisition Branch's guidance and oversight, execution of sound contracting techniques and

approaches, and the agency's current procurement application. OIG reviews also show that the FTC faces challenges in retaining and managing a fully competent agency cadre of Contracting Officers (COs) and Contracting Officer's Representatives (CORs). Some CORs lack general knowledge of the procurement process and are unaware of the most appropriate contract vehicle. CORs also have difficulty gathering and drafting requirements for contract solicitations, including proper performance metrics that measure progress toward satisfaction of contract objectives, and addressing poor contractor performance. Consequentially, the FTC risks poor contractor performance; losing money on unnecessary or poorly written contracts; and costly contract modifications and other adverse consequences from contracts that are not adequately written and deficient products and services delivered.

Significant turnover in the staff responsible for administering, supporting, and overseeing the agency's acquisition program has disrupted the contract management process. For example, in FY 2015, two veteran COs departed; and the FTC hired a new Chief Acquisition Officer, four new COs, and a new vendor to provide contract management support. While staffing changes can introduce opportunities for improvements in process and program re-design, the staff "churn" experienced at the FTC poses operational risks due to lack of program continuity and consistency. This risk is particularly evident for CORs, who collaborate with COs during the requisition, contract award, and contract administration processes. Different COs may have different interpretations of the Federal Acquisition Regulations (FAR) and the COR role in monitoring contract performance. The absence of clear and timely communication of procedures, practices, and roles can result in inconsistent and ineffective contract management. Further complicating the contract management challenge is that the contract administration support application is not integrated with FTC's financial system and does not provide contract funding or status visibility to the COR or CO. Without such capabilities, FTC contract administration staff must manually track significant contract events such as period of performance warning and end dates, and funding status and "burn rates."

To address this challenge, in FY 2016, the FTC will begin a multi-year process to fully integrate its procurement and financial systems. The new system is intended to integrate the FTC's acquisition and financial systems to provide improved data transparency and help the agency realize its Strategic Plan Objective 3.1, to "optimize resource management and infrastructure." Successfully updating agency processes, policies and guidance for the new system and training staff in effective use of the expanded capabilities will be an ongoing challenge.

Agency Progress in Addressing the Challenge

While the FTC has had significant turnover in contracting staff and support in FY 2015, the Financial Management Office (FMO) has been working diligently to improve the agency's procurement program. Under its new leadership, FMO's Acquisitions Branch is rebuilding and specifically directing its efforts to delivering clear and consistent guidance and advice and more robust customer support through: 1) improved COR education; 2) improved management controls in, and the restructuring of, the Acquisitions Branch; 3) revised policy and procedures; and 4) implementation of an electronic contract life cycle support system.

For example, Contracting Officer Representative (COR) education is a priority for both FMO management and the Chief Acquisitions Officer (CAO). FMO hosted required COR training in July 2015 and will provide quarterly training going forward. Training topics will address current COR needs and be directed towards maturing the FTC COR community's knowledge base. Easy to access COR resources are being developed on key procurement business processes, similar to the resources that FMO provided on expert witnesses in 2014. FMO is committed to tracking COR information manually until the Contract Lifecycle Module (CLM), discussed more fully below, is online in FY 2016. CLM will allow COR information to be electronically updated and will provide reports of current CORs.

The new CAO has built considerable structure around the contract file documentation and award review processes, ensuring a level of consistency and that staff are held accountable to all appropriate FAR standards. In FY 2015, the Acquisitions branch was restructured into three teams, focused around key customers – the Administrative Services Office, the Office of the Chief Information Officer, and the Bureaus and Offices, with a separate dedicated Contracting Officer to support contracts for expert witnesses. Team leads and their colleagues meet weekly with their customers so that there is a constant, free-flow of information throughout the procurement process. Additionally, the Acquisitions Branch is contracting with an acquisition support provider to provide liaisons to each of its major customers. The liaisons will provide guidance on the acquisition process; ensure proper documents necessary for contracting are in place; assist customers with initiating contract actions; and usher the acquisition through the process so that both the Acquisitions Branch and the customer maintain visibility and confidence throughout the entire process. This too should help increase COR confidence in, and knowledge about, the acquisition process.

The CAO has directed a review of all policy and that new policies and procedures consistent with the latest FAR provisions and other relevant federal regulations be drafted as required. When completed, the Acquisitions Branch will have standardized policies and procedures that will govern and simplify contracting actions for all contracting officers and CORs. This standardization will give consistency to all acquisition actions, which in turn will make operations more efficient and ensure compliance with federal regulations and guidance. The CAO also conducted a thorough review of all staff performance objectives to ensure that required annual training is completed and staff obtains additional professional development opportunities to stay current and to improve their overall acquisition knowledge and performance.

As noted above, the FTC is working with the agency's shared service provider, IBC, to implement a contract lifecycle management module for FTC's financial system. CLM will greatly improve the way the FTC buys goods and services, routes requisitions, and administers and reports contract information. It will provide much needed visibility to CORs into the funding status of their contracts. A dedicated project manager will work with FMO, IBC, and agency stakeholders to help manage CLM's implementation and document needed business process changes. FMO will also obtain a third party, independent verification and validation of CLM's implementation to ensure that it meets FTC's requirements. Finally, FMO has assembled an agency-wide workgroup to help update business processes, gather requirements, and train others. The workgroup,

composed of agency employees familiar with submitting requisitions and the acquisitions process, is poised to help ensure a smooth and positive transition to the new system.

The above-noted changes have taken time to put in place, and while a number of these efforts are still ongoing, now that the branch is right-sized, customer-focused, and providing more consistent guidance, we are confident that the agency' procurement program is positioned for success.

4. Stabilizing the Agency's eDiscovery Support System

The FTC maintains a litigation support platform that functions as an eDiscovery Support System (eDSS) for legal processing and legal review. Through a contract award in 2012, the eDSS was intended to enable the FTC's two litigating Bureaus – Competition and Consumer Protection – and the FTC's eight remote Regional Offices to store, process, review, and tag large sets of data for its cases. Competition case teams use the platform in their litigation efforts challenging mergers and acquisitions and anticompetitive conduct. Consumer protection case teams use the eDSS to support enforcement of federal consumer protection laws.

The eDSS was not effectively integrated into the FTC technical infrastructure and FTC business practices. As a result, it has experienced significant management and technical deficiencies, including cost overruns and persistent system latency. The persistent technical issues impede users' ability to rely upon the platform to move between documents or retrieve data – all critical requirements in deadline-driven litigation.

The eDSS challenges are complicated by the FTC's inability to perform basic troubleshooting and root cause analyses. For example, the lack of appropriate technical tools and lack of understanding of concurrent processing and system logging restrict the FTC from effectively evaluating workload impacts due to difficulties in determining the number of concurrent users. Echoing other management challenges the OIG identified this year, there is no formal process for problem follow-up, monitoring the aging of trouble reports, or oversight of actions taken and/or required to assess and resolve the eDSS problems.

The eDSS was intended to replace six obsolete legacy systems, process four terabytes of data daily (Bureau cases can each require a range of 300 GB to 4 TB of storage), and permit access for 150 concurrent-license users. Due to persistent outages and functionality issues, these objectives have not been achieved after three years of contract performance. FTC litigation teams have adapted as best they can to continue to bring successful cases.

Stabilizing the eDSS is essential to enabling the FTC to accomplish its competition and consumer protection missions. The FTC needs to support "big data" analyses, especially as the volume of data that must be processed continues to increase and analytical approaches become more complex. In FY 2016, the OIG will complete an evaluation of the root causes of the eDSS performance and management issues. The evaluation will contain recommendations to mitigate performance risk with the current eDSS platform and to prevent similar occurrences in future efforts to modernize and enhance the FTC technological case and data analysis capabilities.

Agency Progress in Addressing the Challenge

The OCIO is actively working on improving the performance and stability of the eDiscovery Support System (also known as EDSS). After continued performance issues in June 2015, OCIO prepared an after-action report (AAR) documenting lessons learned, root cause analysis, and recommendations for future improvements. The AAR will be presented to the IT Governance Board in October 2015 for review and approval of the recommended course of action. The recommended course of action includes increasing resources to support the application, implementing better performance monitoring and issue tracking, and streamlining the acceptance testing process to decrease the time and effort needed to perform upgrades and software patches needed to fix code errors and security vulnerabilities (hotfixes). The additional resources requested will provide OCIO with the expertise needed to troubleshoot performance problems, perform timely upgrades and patches, and implement necessary changes to the configuration to improve performance and functionality.

The move to implement timely upgrades and patches are critical to improving EDSS's performance. These upgrades are critical to ensuring errors or bugs in the application code are fixed before causing major performance degradation. To streamline the process for implementing upgrades and hotfixes, the OCIO is recommending moving the development and acceptance test functions for EDSS to a testing platform in the production environment. This will provide a dedicated development and testing environment without the constant configuration changes in the standard development and testing environment, which will lead to faster deployment of bug fixes and patches. The OCIO is also proposing, as part of the AAR, a service-level agreement to require implementing hotfixes 14 calendar days after release and upgrades 30 calendar days after release of the first service pack.

As the OCIO continues to troubleshoot and make improvements to the EDSS application and the underlying infrastructure, system performance will be closely monitored to validate whether the configuration changes are actually improving performance. In support of monitoring, OCIO will conduct an overall analysis review of the As-Is environment for EDSS, document configuration baselines, and establish performance benchmarks for future EDSS updates. Additionally, the OCIO will define infrastructure performance metrics for a number of parameters to include server and network utilization. This will assist the OCIO in further determining whether performance issues arise from the application or the infrastructure.

Looking toward the future, the OCIO will begin an analysis of alternatives for the EDSS application to begin preparation for the expiration of the EDSS contract in FY 2017. As part of this alternative analysis, the OCIO and business owners in the bureaus will analyze alternative applications, including externally hosted solutions, and determine whether EDSS is still the best option for the agency's current and future litigation support, eDiscovery, and "big data" requirements.

5. Ensuring Compliance with Digital Records Management Requirements

In November 2011, the President signed a Presidential Memorandum, *Managing Government Records*, instituting a government-wide effort to reform records management policies and practices. In August 2012, OMB and the National Archives and Records Administration (NARA) issued a "Managing Government Records Directive" that requires "to the fullest extent possible, [federal] agencies eliminate paper and use electronic recordkeeping." We must address these challenges while using the opportunity to develop a 21st-century framework for the management of Government records.

The OMB/NARA Directive requires federal agencies to make several changes in records management processes. The Directive states: "By December 31, 2016, Federal agencies must manage all email records in an electronic format. Email records must be retained in an appropriate electronic system that supports records management and litigation requirements (which may include preservation-in-place models), including the capability to identify, retrieve, and retain the records for as long as they are needed. Beginning one year after issuance of this Directive, each agency must report annually to OMB and NARA the status of its progress toward this goal." The Directive also states: "By December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format."

The Directive has significant implications for FTC operations. It requires a shift from paper to digital records wherever possible, and to provide appropriate training to FTC staff. The FTC will need to reconsider its records organizations procedures from the authoring and creation of records; to the methods and tools used to acquire, store, track, and retrieve them; and, finally, to their disposal.

The FTC Congressional Budget Justifications for FY 2015 and FY 2016 set forth the same strategies for an FTC transition to electronic information resource management: "(1) Developing an agency-wide information governance policy that provides enterprise-level standards for file structures for organizing information, mandatory and optional metadata (searchable information about the document), document naming conventions, access restrictions, and retention rules and triggers. (2) Implementing an Enterprise Content Management System (ECMS) that staff will use to draft, collaborate on, and finalize work, including consumer protection and competition case filings. The ECMS will enable us to maintain agency records in a secure electronic format for the required retention period and to transfer permanent agency records to the National Archives and Records Administration (NARA) [in an electronic format]." Enterprise Content Management System electronic information resource management with the following: an agency-wide information governance policy that provides enterprise-level standards for structured, organized information; mandatory and optional metadata; uniform document naming conventions; access restrictions; and retention rules and triggers. Such a strategy will enable the FTC to maintain agency records in a secure electronic format for the required retention period, and transfer permanent agency records to NARA as necessary.

To fully comply with the OMB/NARA directive and other legal requirements regarding electronic recordkeeping, the transition to digital records management will require the FTC's continued focus in FY 2016. In particular, the Records and Filings Office must provide guidance and enhanced search capacities for electronic documents. The agency also must continue to train staff in identifying and labeling federal records (including emails), as well as proper and NARA-compliant retention and disposition of records.

Agency Progress in Addressing the Challenge

NARA approved a new comprehensive records retention schedule for the FTC in 2012. This records retention schedule is media neutral and thus gives the FTC the legal authority to maintain its federal records in electronic format. The transition to maintaining agency records in electronic format is well underway. FTC staff currently store and access electronic information in shared network drives, following the FTC's Shared Network Space policy that was established in 2006. This policy establishes a high-level folder structure and enhances the ability to control access privileges to information. In 2013, FTC's Records and Filings Office (RFO) issued guidance to agency staff that federal records – including email records – can be stored on shared drives as part of the matter file. Use of shared drives to store records is consistent with the agency's business process and with NARA Bulletin 2012-02 (December 6, 2011), on "Guidance on Managing Content on Shared Drives," and meets the OMB/NARA Directive requirement to manage all email records in an electronic format by 2016. In 2015, RFO developed a new Managing Your Electronic Files tip sheet that provides additional guidance to agency staff on managing records (including email) in electronic format.

As part of the transition to maintaining agency records in electronic format, the FTC continues to use our Electronic Recordkeeping Certification Review (ERCR) process to evaluate recordkeeping requirements for existing and new systems. RFO has certified two systems to house permanent electronic records – the Matter Management System 2 and the E-Filing system for FTC administrative litigation. In FY 2015, RFO enhanced the E-Filing system to include non-public filings, electronic service of filings, and an electronic docket. These enhancements make the FTC administrative litigation process and its official records virtually fully electronic.

RFO is working with agency stakeholders to develop information governance for FTC records. This includes file structures, metadata, naming conventions, access restrictions, and retention rules and triggers. The FTC plans to utilize an Enterprise Content Management System (ECMS) to maintain agency records for the required retention period and to transfer permanent agency records to NARA in electronic format. The FTC plans to incorporate the management of email records in the ECMS. The ECMS will provide enhanced search capacities for electronic documents and meet the OMB/NARA Directive requirement to manage permanent electronic records electronically by 2019. In FY 2015, the agency continued planning for transition to an ECMS, as part of FTC's overall IT modernization strategy.