TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

# *Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution*

**October 30, 2015**

**Reference Number: 2016-20-002**

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

**Redaction Legend:**
2 = Risk Circumvention of Agency Regulation or Statute
10 = Trade Secrets or Privileged or Confidential Commercial or Financial Information

*Phone Number / 202-622-6500*
*E-mail Address / TIGTACommunications@tigta.treas.gov*
*Website / http://www.treasury.gov/tigta*

**MEASURABLE AGREEMENTS ON SECURITY CONTROLS ARE NEEDED TO SUPPORT THE ENTERPRISE STORAGE SERVICES SOLUTION**

# Highlights

**Final Report issued on October 30, 2015**

Highlights of Reference Number: 2016-20-002 to the Internal Revenue Service Chief Technology Officer.

## IMPACT ON TAXPAYERS

The Enterprise Storage Services (ESS) Program is sponsored by the IRS Storage Program Management Office. This office delivers data storage services to Enterprise applications at IRS facilities through deployment of tiered storage, encrypted backup/recovery, and data replication strategies that enable high-performance systems operations, business continuity, and dynamic and secure disaster recovery. The IRS estimates that its new "Storage-As-a-Service" approach will save millions of dollars by providing better utilized resources. With the ESS contract, the IRS's initial estimates were for a **********10********* **********10**********. The new ESS environment stores IRS data, including taxpayer and other sensitive data.

## WHY TIGTA DID THE AUDIT

The overall objective was to assess the efficiency and effectiveness of the IRS's ESS Program by considering progress toward established goals and the risk mitigation approach for the enterprise-wide cloud storage services that support IRS systems and information technology operations.

## WHAT TIGTA FOUND

The IRS has reported cost savings with its migration of production data into the ESS storage environment since March 2013. Since the Unisys contract began, estimated cost savings for **********10********** ******10*****. These savings, under the ESS Program, represent approximately ****10***of the IRS's estimated ***10*** cost savings for the new Managed Service approach.

However, TIGTA found that more detailed contractual agreements are needed to support the ESS Program with data security controls including security monitoring and incident management. Clear agreements between the IRS and the ESS contractor would better ensure adequate preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. Also, the Service Level Objectives established under the current contract do not clearly stipulate time frames for the contractor to mitigate losses and resecure the ESS environment should a data breach occur.

## WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS Chief Technology Officer: 1) modify the ESS contract to include measurable Service Level Agreements based on a complete risk assessment and security plan for the ESS Program and 2) address specific risks affecting IRS systems related to ESS security monitoring and incident management.

The IRS disagreed with both recommendations, stating that the ESS provides disk storage as one component of a larger, multilayered infrastructure. Risk and security of all data, including access to the data in addition to IRS incident management and security monitoring, are performed at the General Support System and Application layers using IRS standard practices and processes.

TIGTA believes that risk factors associated with contract responsibilities and ownership of ESS data storage devices should be considered under the ESS Program. IRS policy requires risk management for all infrastructure equipment capable of storing or transmitting data. However, a risk assessment has not been conducted, and the security plan is not complete. The IRS has not provided TIGTA with verification that security controls to address specific ESS risks have been considered at the General Support System and Application layers. The ESS contract does not include or reference a detailed process to guide security monitoring and overall incident management controls.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 30, 2015

**MEMORANDUM FOR** CHIEF TECHNOLOGY OFFICER

**FROM:** Michael E. McKenney
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution (Audit # 201520016)

Attached for your review and comments is the subject audit report. The overall objective of this review was to assess the efficiency and effectiveness of the Internal Revenue Service's (IRS) Enterprise Storage Services Program by considering progress toward established goals and the risk mitigation approach for the enterprise-wide cloud storage services that support IRS systems and information technology operations. This audit is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenges of Modernization, Achieving Program Efficiencies and Cost Savings, and Security for Taxpayer Data and IRS Employees.

Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

# *Table of Contents*

# *Abbreviations*

| | |
|---|---|
| ESS | Enterprise Storage Services |
| FY | Fiscal Year |
| IRS | Internal Revenue Service |
| NIST | National Institute of Standards and Technology |
| SLOs | Service Level Objectives |
| SP | Special Publication |

# Background

The Enterprise Storage Services (ESS) Program is sponsored by the Internal Revenue Service (IRS) Storage Program Management Office. The Storage Program Management Office's mission is to deliver world-class data storage services to enterprise applications at IRS facilities through deployment of tiered storage, encrypted backup/recovery, and data replication strategies that enable high-performance systems operations, business continuity, and dynamic and secure disaster recovery. The Storage Program Management Office governs and facilitates delivery of the ESS Program. The Data Management Services and Support Division in the Enterprise Operations organization manages the ESS Program. The ESS Program provides enterprise storage for IRS data, including taxpayer and other sensitive data.

In December 2010, the U.S. Chief Information Officer released the *25 Point Implementation Plan to Reform Federal Information Technology Management*. The document called for a shift to a "Cloud First" policy where cloud services can be deployed rapidly and shared solutions will result in substantial cost savings, allowing agencies to optimize spending and to reinvest in their most critical mission needs.[1] Then, in February 2011, the U.S. Chief Information Officer published the *Federal Cloud Computing Strategy*, requiring Federal agencies to evaluate safe, secure cloud computing options before making any new information technology investments.[2]

Also, the September 2011 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, states that cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, *e.g.*, networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction. Several benefits of cloud computing are increased scalability, on demand services, energy efficiency, resources pooling, and metered services. The cloud computing technology is comprised of four deployment models:

- *Community Cloud* – The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns, *e.g.*, mission, security requirements, policy, and compliance considerations. It may be managed by the organizations or a third party and may exist on premises or off premises.
- *Hybrid Cloud* – The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized

[1] *25 Point Implementation Plan to Reform Federal Information Technology Management*, published on Dec. 9, 2010, by Kundra, Vivek.
[2] *Federal Cloud Computing Strategy*, published on Feb. 8, 2011, by Kundra, Vivek.

or proprietary technology that enables data and application portability, *e.g.*, cloud bursting for load balancing between clouds.

- *Private Cloud* – The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premises or off premises.
- *Public Cloud* – The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

In February 2012, the Federal Chief Information Officer Council and the Chief Acquisition Officers Council published *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*. This document provides Federal agencies more specific guidance to effectively implement the Cloud First policy and move forward with the Federal Cloud Computing Strategy.

Figure 1 demonstrates that the legacy IRS storage environment was largely configured, aligned, and managed in a stovepipe fashion. The ESS contract states that this structure had no ability to manage storage assets across the enterprise. Storage had to be acquired, allocated, and managed on a project-by-project basis. This proved to be an inflexible solution that resulted in low utilization and usage inefficiencies. In Fiscal Year (FY) 2009, the IRS began researching and analyzing its storage costs over a four-year period and determined that it had paid approximately $92 million to purchase support storage for all IRS systems.

***Figure 1: **********2*************

**********
**********
**********
**********
**********
**********
**********2**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********

In June 2012, the ESS Program was established and the Unisys Corporation (Unisys) was awarded the ESS contract to work with the IRS to implement a private cloud-based data storage solution that will:

- Transfer ownership of the IRS existing storage arrays.
- Enable tiered, virtualized high-performance storage.
- Provide faster storage acquisition and allocation.
- Result in significant cost savings based on actual data stored rather than total capacity.

The ESS contract **********10********** **********10**********. The IRS exercised the FY 2015 one-year renewable option on June 29, 2015.

According to the ESS contract, Unisys will plan, design, build, deploy, and maintain a new storage environment under the guidance and oversight of the IRS Storage Program Management Office, but Unisys will not manage the Storage Area Network infrastructure or Storage Area Network virtualization. The new storage environment will have agile processes in which continual improvements are rapidly deployed, storage and retrieval of data are optimized, and flexibility for growth and innovation are integrated into the solution.

The ESS contract defines four data storage classes for the IRS as follows:

- **Platinum –** The Platinum class is service to support the most demanding transactional workloads. It guarantees high availability and the ability to support extreme computational performance.
- **Gold –** The Gold class is a service that can support high speed, high reliability, and the ability to service many data consumers simultaneously. The Gold class is used for shared critical data and large, computationally intensive applications.
- **Silver –** The Silver class is a service that is highly performing, configurable, and modular. This class is suitable for most servers and operating loads. It may support fewer performance-driven applications simultaneously or provide storage for many capacity-driven applications.
- **Bronze –** The Bronze class is a service to provide moderate performance at a reduced cost per gigabyte. It is configurable, modular, and suitable for large-capacity data stores for most servers.

According to the ESS contract, the Unisys solution will create a private, cloud-based data storage environment on IRS premises. The IRS plans for the Unisys solution to be available to IRS business units/functions for which storage is immediately available as needed and paid for only as used. The IRS estimates that its new "Storage-As-a-Service" approach will save millions of

dollars by providing better utilized resources. With the ESS contract, the IRS's initial estimates were for a **********10**********.

Figure 2 depicts the ESS Managed Storage Services solution as an enterprise-wide view of storage resulting in improved planning, management, and sharing of resources to address all objectives and requirements.

***Figure 2: **********2*************

**********
**********
**********
**********
**********
**********2**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********
**********

This review was performed at the IRS's Information Technology organization in New Carrollton, Maryland, during the period February through July 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions

based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

# Results of Review

## The Enterprise Storage Services Program Has Reported Cost Savings

The Infrastructure Executive Steering Committee provides governance for IRS information technology infrastructure plans, activities, and investments of the Infrastructure Architecture and Engineering Division, including the ESS Program. For FY 2013, the committee approved funding for the new private cloud-based storage solution. Subsequently, funding for the ESS solution has been provided through the Operating and Maintenance budget and other projects.

Since March 2013, the IRS has been migrating production data into the ESS storage environment. The IRS provided the Treasury Inspector General for Tax Administration with planned and actual costs and cost savings for the Managed Service approach for ESS data storage versus the cost of the legacy IRS data storage environment. Figure 3 summarizes cost savings information[3] available for the ESS Program.

[3] Verification of the accuracy and completeness of the cost data provided was outside the scope of this audit.

### *Figure 3: Enterprise Storage Services Cost Information*

| Actual Cost to Operate Legacy IRS Data Storage Environment | Ref.[4] | Amount Reported |
|---|---|---|
| Five-year cost (FYs 2008–2012) to operate the legacy IRS data storage environment | | $ 92 million |
| Average cost per year ($92 million / five years) | | $ 18.4 million |
| Average cost for three years ($18.4 million times three years) | | $ 55.2 million |
| | | |
| **Cost Comparison** | | |
| Estimated cost to operate the legacy IRS data storage environment for 10 years | *10* | *****10**** |
| Estimated cost to use the Managed Service approach for data storage for 10 years | *10* | *****10**** |
| Estimated cost savings to use the Managed Service approach for data storage (A - B) | *10* | *****10**** |
| | | |
| **Actual and Planned Costs for the Managed Service Approach for Data Storage** | | |
| Actual costs (July 2012 – June 2015) | *10* | *****10**** |
| Planned costs (July 2015 – September 2015) | *10* | *****10**** |
| Total actual costs + planned costs (D + E) | | *****10**** |
| | | |
| **Cost Savings[5]** | | |
| FY 2011 – FY 2014 | *10* | *****10**** |
| FY 2011 | *10* | *****10**** |
| FY 2012 – FY 2014 (F – G) | *10* | *****10**** |
| Percentage of cost savings goal (H/C) | *10* | *****10**** |

*Source: IRS Strategic Supplier Management Program.*

[4] Ref. represents a reference point.
[5] The IRS did not report ESS cost savings for FY 2015.

## More Detailed Contract Specifications Are Needed to Ensure Sufficient Data Security Controls Under the Enterprise Storage Services Program

Best practices[6] for information technology service contracts include Service Level Agreements to define acceptable service levels and measurable terms under the contracts. Service Level Agreements are necessary between a cloud service provider and customer to contractually agree upon the acceptable service levels expected from a cloud service provider. The ESS contract includes what are termed as Service Level Objectives (SLOs).[7]

The Treasury Inspector General for Tax Administration assessed the IRS's progress toward established goals and its risk mitigation approach for the enterprise-wide cloud storage services supporting IRS systems and information technology operations. Our assessment found that the ESS contract and supporting documents, including SLOs, do not reflect a current and complete risk assessment or security plan for the ESS Program. Further, the IRS had not completed annual contractor system security reviews that are required by the ESS contract. These types of management controls provide essential information to determine the adequacy of ESS data security. They also provide necessary information to determine appropriate courses of action in response to identified risks. By not completing these important risk mitigation steps, the IRS has not yet identified baseline security controls or control enhancements to ensure data security and integrity for IRS data stored within the ESS environment.

Further, the ESS contract SLOs do not clearly define important aspects of risk mitigation controls needed to protect data under the ESS Program. As discussed below, the SLOs have not clearly defined how performance is guaranteed in key areas, including controls for security monitoring and incident management required for IRS systems. More detailed Service Level Agreements for security monitoring and incident management would strengthen the IRS's ability to ensure that the ESS contractor sufficiently monitors data security, provides timely notification of any failures to meet measurable agreements under the contract, and demonstrates evidence that problems have been resolved or mitigated as expected. Without such agreements, the IRS may be unable to determine ESS Program compliance with applicable policies and procedures that protect sensitive data.

[6] Chief Information Officer Council and Chief Acquisition Officers Council publication, *Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*, dated June 2012.
[7] The SLOs are agreed as a means of measuring the performance of the service provider. The SLO may be composed of one or more quality-of-service measurements that are combined to produce the SLO achievement value.

## Security monitoring and incident management

Internal Revenue Manual 10.8.1[8] requires assessment teams to monitor the security controls in an information system on an ongoing basis. In addition, NIST 800-53 (Revision 4) states that continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.

Internal Revenue Manual 10.8.1 also requires personnel to report suspected cybersecurity incidents to the IRS Computer Security Incident Response Capability, the enterprise-wide reporting entity, within specified time frames. Further, Federal agencies must ensure that contracts with cloud service providers include cloud service provider liability for data security.

The ESS contract states that the contractor shall maintain procedures for detecting, reporting, and responding to security incidents, and mitigating risks associated with such incidents, before substantial damage is done to Federal information or information systems. The contractor shall immediately report all computer security incidents that involve IRS information systems to the IRS Computer Security Incident Response Capability. Any theft or loss of information technology equipment with Federal information/data must be reported within one hour of the incident to the Computer Security Incident Response Capability.

However, the ESS contract and supporting documents do not contain sufficient detail regarding: a) preparation; b) detection and analysis; c) containment, eradication, and recovery; and d) post-incident activity. Further, the SLOs do not establish time frames for the contractor to mitigate losses and resecure the ESS environment should a data breach occur.

Our review also found that, under the ESS Program, the IRS has not fully considered risk mitigation for applications and business functions that rely on the data storage services provided by the ESS solution. For instance, the ESS SLOs do not clearly define important aspects of security monitoring and incident management controls that are required to protect data within the ESS environment. Moreover, the ESS Program does not maintain an association between the data stored in ESS and specific security requirements for IRS systems and applications. During our review, Unisys employees informed us that they had recently begun collaborating with the IRS Cybersecurity organization on an integrated enterprise continuous monitoring program in June 2015.

According to the NIST,[9] security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The IRS informed us that it stores and manages its data within ESS containers. The ESS Program does not manage or have access to the data; it owns and only provides access

[8] IRM 10.8.1 (Dec. 23, 2013).
[9] NIST 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, (April 2013).

to the storage. ESS officials explained that IRS system and application owners manage and retain responsibility for the data held by the new storage solution. However, the ESS Program has not performed a risk assessment that considers IRS system and application requirements for data security and privacy. As a result, the IRS has not yet ensured that operational controls within the new data storage environment are effective for the systems and applications relying on this enterprise-wide private cloud-based data storage solution.

These conditions further indicate that all controls required for IRS systems were not fully considered with the ESS storage solution. Consequently, it is essential that the ESS Program more clearly specify acceptable and agreed-upon service levels for security monitoring and incident management, including roles, responsibilities, and measurable results under the contract. Moreover, by strengthening the service management approach for the ESS Program, the IRS could better ensure the long-term success and realization of expected benefits with this major information technology initiative.

## Recommendations

The Chief Technology Officer should ensure that:

***Recommendation 1:*** The ESS contract is modified to include measurable Service Level Agreements based on a complete risk assessment and security plan for the ESS Program.

> ***Management's Response:*** The IRS disagreed with this recommendation for the ESS contract. However, it will take the recommendation under advisement for managed service contracts that handle IRS business or application data. The IRS stated that, similar to a device, the ESS provides disk storage as one component of a larger, multilayered infrastructure. The ESS does not handle, manipulate, or access any IRS business data. The ESS simply provides the containers (disk drives) on which the data are stored. Risk and security of all data, including access to the data, is managed by the IRS at the General Support System and Application layers not at the storage device or disk drive level. Data are handled by business applications and are covered under the Federal Information System Management Act operational, management, and technical controls at the application layer.
>
> ***Office of Audit Comment:*** During the audit, the IRS referred to ESS as a private cloud-based data storage solution. The ESS contract provides for a virtual storage solution that includes infrastructure components, or storage devices, that contain most of IRS data including sensitive data. Risk factors associated with contract responsibilities and ownership of ESS data storage devices should be considered under the ESS Program. IRS policy also requires risk management for all infrastructure equipment capable of storing or transmitting data. However, an ESS Program risk assessment has not been conducted, and our review found that the ESS Program security plan is not complete. Further, the IRS has not provided us with verification that security controls to

address specific ESS risks have been considered at the General Support System and Application layers. Our review also found that measurable Service Level Agreements are considered a best practice that can help Federal agencies manage risks within all types of cloud-based information technology solutions.

***Recommendation 2:*** The ESS Program sufficiently addresses specific risks affecting IRS systems related to ESS security monitoring and incident management.

***Management's Response:*** The IRS disagreed with this recommendation and stated that the ESS Program has no role in application, server, or infrastructure security monitoring and incident management. IRS incident management and security monitoring are performed at the General Support System and Application layers using IRS standard practices and processes. ESS disk drives are a component of a larger infrastructure in which monitoring occurs at the server and application level, not at the storage device or disk drive level.

***Office of Audit Comment:*** The ESS data storage devices may be vulnerable to direct security or privacy threats including internal threats that could result in security breaches. For instance, a malicious attack on the storage devices could result in: (a) an ESS device and service disruption which leads to the unavailability of the IRS data and systems, (b) a data breach of IRS data including sensitive data, or (c) compromise of IRS data integrity. Our review found, however, that the ESS contract does not include or reference a detailed process to guide all security monitoring and overall incident management controls within the new private cloud-based data storage solution.

## Appendix I

# *Detailed Objective, Scope, and Methodology*

The overall audit objective was to assess the efficiency and effectiveness of the IRS's ESS Program by considering progress toward established goals and the risk mitigation approach for the enterprise-wide cloud storage services that support IRS systems and information technology operations. To accomplish our objective, we focused on the following known risk areas identified during planning:

I. **Management Controls:** Evaluated the adequacy of the management controls, including key milestones and the risk mitigation approach for the ESS Program.

   A. Identified the ESS Program's approach for managing its cloud computing solution in accordance with Federal guidelines and other applicable guidance.

II. **Operational Controls:** Evaluated the adequacy of the operational controls, including contract activities for information technology services under the ESS Program.

   A. Evaluated the adequacy of the contract administration for the ESS Program.

III. **Configuration Management:** Evaluated the adequacy of the general controls, including information technology configuration management practices for services provided under the ESS Program.

   A. Evaluated the risk mitigation activities of the ESS Program's virtualization implementation.

IV. **Security Management:** Evaluated the adequacy of the general controls, including information technology security management practices, for services provided under the ESS Program.

   A. Evaluated the risk mitigation activities for the ESS solution in the areas of Identity Management and Access Control Management.

### ***Internal controls methodology***

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Internal Revenue Manual and related cloud computing policies and procedures of the ESS environment. We evaluated these controls by interviewing IRS management and staff; reviewing policies and procedures outlined in Internal Revenue Manual, NIST, and other applicable guidance; and reviewing relevant

supporting documentation. Documents reviewed include the ESS contract with Unisys, ESS Project Charter, ESS Project Management Plan, and other documents that provided evidence of whether the IRS is adequately managing risks for the ESS Program.

## Appendix II

# Major Contributors to This Report

Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director
Suzanne Westcott, Audit Manager
Lynn Ross, Lead Auditor
Hung Dam, Senior Information Technology Specialist
Allen Henry, Program Analyst
Charlene Elliston, Senior Auditor
Wallace Sims, Senior Auditor

## Appendix III

# *Report Distribution List*

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief, Agency-Wide Shared Services OS:A
Deputy Chief Information Officer for Operations OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Associate Chief Information Officer, Strategy and Planning OS:CTO:SP
Director, Data Management Services and Support OS:CTO:DM
Director, Procurement OS:A:P
Director, Business Planning and Risk Management Division OS:CTO:SP:RM
Director, Storage Program Management Office OS:CTO:DM:SPMO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Director, Business Planning and Risk Management Division OS:CTO:SP:RM

## Appendix IV

# *Management's Response to the Draft Report*

CHIEF TECHNOLOGY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

SEP 22 2015

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Data Storage as a Service - #201520016

Thank you for the opportunity to review your draft audit report and to provide our comments as it relates to our Enterprise Storage Services (ESS) project. We appreciate your acknowledgment of the $17.7 million cost savings the program has delivered thus far.

Since ESS is merely Storage-as-a-Service and not a full Infrastructure-as-a-Service as the report implies, the ownership, management, and protection of IRS business data is performed by IRS applications and covered under appropriate Federal Information Security Management Act (FISMA) controls. All business data contained within the ESS storage arrays can only be accessed by IRS applications and computing infrastructure that are managed and operated by IRS personnel. While we strongly believe in the value of risk assessments, security plans, and a robust incident management process, we do not agree that your proposed recommendations are applicable to the current ESS contract. In particular, your audit report does not differentiate between *disk storage containers* and the *management and protection of the data within those containers*. This distinction is fundamental as the ESS contract provides disk storage containers that operate in exactly the same way as they did under the IRS managed Storage Area Networks (SANs) that ESS replaced.

Your audit report focuses on the security provisions of the ESS contract assuming that the storage capabilities provided by the ESS contract should or must provide the complete range of security capabilities separate and apart from the IRS-owned and managed infrastructure and business applications. IRS asserts that any security assessment of the ESS capabilities must consider the security layers deployed for all IRS applications and data. Since your audit report does not state that you reviewed IRS's General Support System or Application security documentation, it includes no statements about the completeness or adequacy of the security controls, monitoring or incident management capabilities over IRS business data referenced in these important security documents. As a result, it does not show how the IRS has responded to preparation; detection and analysis; containment, eradication, and recovery; and post-

incident activity to mitigate losses and re-secure the ESS environment should a business data breach occur.

Based on the role of ESS as a provider of storage and the adequacy of IRS security controls for IRS data, the IRS contends that the ESS contract requires the appropriate level of security and incident management. Specifically, the contract contains an Interconnection Security Agreement (ISA). The ISA is the formal, contractually binding document that specifies the security obligations and contains the System Security Plan for the On Command application that is used to manage and monitor the storage containers. The SSP is current and is going through the annual update process to reflect the most current NIST guidelines. Additionally, both the ISA and SSP follow IRS policy which requires a 1-hour response for incident management. Specific risk assessments of server and application controls for the data stored in the ESS containers can be found in the applicable General Support System and Application systems security plans as required by FISMA.

Lastly, the IRS respectfully disagrees with the assertion that "by strengthening the [security] service management approach for the ESS Program, the IRS could better ensure long-term success and realization of expected benefits with this major information technology initiative." The report does not provide any specific evidence to support this statement, such as citing any deficiencies with non-security related service level objectives (SLOs) or specific performance metrics. The report also provides no specific examples of the implied dependencies of the "realization of expected benefits of the initiative" and proposed security SLOs. To the contrary, at least 66% of the cost benefits expected over the 10 year contract were realized in the first 3 years of the project. This does not include the intangible IRS benefits of time, flexibility, availability, and simplicity to deliver storage capacity.

We are committed to continuously improving our information technology systems and processes. We value your continued support and the assistance and guidance your team provides. In this regard, we acknowledge our commitment to the federal government's "Cloud First" policy and appreciate the information you provided to help us as we pursue our cloud computing strategies and put in place sound contracts for cloud computing services. If you have any questions, please contact me at (240) 613-9373 or Joe Sanchez at (202) 215-6152.

Attachment

Attachment

Draft Audit Report – Data Storage as a Service (Audit # 201520016)

**RECOMMENDATION #1:** The Chief Technology Officer should ensure that ESS contract is modified to include measurable Service Level Agreements based on a complete risk assessment and security plan for the ESS Program.

**CORRECTIVE ACTION #1:** The IRS disagrees with this recommendation for the ESS contract. However, IRS will take the recommendation under advisement for managed service contracts that handle IRS business or application data. Similar to a device, the ESS provides disk storage as one component of a larger, multi-layered infrastructure. The ESS does not handle, manipulate or access any IRS business data. The ESS simply provides the container, or the disk drives on which the data is stored. Risk and security of all data, including access to the data, is managed by IRS at the General Support System and Application layers, not at the storage device or disk drive level. Data is handled by business applications and is covered under the FIMSA operational, management, and technical controls at the application layer.

**IMPLEMENTATION DATE #1:** N/A

**RESPONSIBLE OFFICIAL #1:** N/A

**CORRECTIVE ACTION MONITORING PLAN #1:** N/A**RECOMMENDATION #2:** The Chief Technology Officer should ensure the ESS Program sufficiently addresses specific risks affecting IRS systems related to ESS security monitoring and incident management.

**CORRECTIVE ACTION #2:** The IRS disagrees with this recommendation. The ESS project has no role in application, server, or infrastructure security monitoring and incident management. IRS incident management and security monitoring are performed at the General Support System and Application layers using IRS standard practices and processes. ESS disk drives are a component of a larger infrastructure where monitoring occurs at the server and application level, not at the storage device or disk drive level.

**IMPLEMENTATION DATE #2:** N/A

**RESPONSIBLE OFFICIAL #2:** N/A

**CORRECTIVE ACTION MONITORING PLAN #2:** N/A