TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement

September 27, 2021

Report Number: 2021-20-066

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement

Final Audit Report issued on September 27, 2021 **Report Number 2021-20-066**

Why TIGTA Did This Audit

Data at rest encryption refers to protection of data residing on system components from unintended usage by applying encryption technology.

The IRS has initiated a Data at Rest Encryption program to address the need for encryption of sensitive data contained in its computer systems. This Program is preparing for initial deployment of encryption solutions to production systems.

This audit was initiated to evaluate the progress of implementing data at rest encryption at the IRS.

Impact on Taxpayers

The IRS collects, generates and stores large amounts of sensitive taxpayer data, Personally Identifiable Information, and proprietary information. This valuable information is continually at risk of unauthorized access, disclosure, or misuse. In particular, information stored on systems known as High Value Assets is critical for the IRS to be able to conduct its tax administration functions. Consequently, encryption of data at rest is vital to protect taxpayer information and IRS operations.

What TIGTA Found

The IRS maintains a large amount of sensitive data in its computer systems. In order to help secure these data, the Data at Rest Encryption program was initiated to identify available encryption solutions for the more than [redacted] systems containing sensitive information. In Fiscal Year 2020, these systems allowed the IRS to collect close to $3.5 trillion in gross taxes and process more than 240 million tax returns and supplemental documents.

The IRS has made progress to identify and test encryption and key management solutions for use with certain types of systems. However, it has not deployed this technology. TIGTA identified specific program issues that have affected the IRS's ability to meet its goals, delaying the encryption of sensitive data, including data contained on systems classified as High Value Assets.

Specifically, Data at Rest Encryption program personnel did not always follow the Enterprise Life Cycle process for project management. Program management issues have contributed to delays to complete the Program's Integrated Master Schedule and resulted in work related to prior audit recommendations not being prioritized.

Lastly, a prior TIGTA recommendation related to encryption of certain data at rest used by Private Collection Agencies was prematurely closed. The IRS verified that sensitive data were being encrypted by the Private Collection Agencies. However, the IRS was not encrypting data intended for Private Collection Agencies on its own production systems.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that the Data at Rest Encryption program follows Enterprise Life Cycle requirements; the established process for creating an Integrated Master Schedule is followed and verify that current schedule information is accurate; there is adequate management oversight of the Program, including following established processes; and data at rest is encrypted prior to being transferred to Private Collection Agencies.

The IRS agreed with all of our recommendations. The IRS plans to ensure the Enterprise Life Cycle requirements are followed; the established process for creating and baselining the Integrated Master Schedule is followed and the existing schedule information is accurate; and the Data at Rest Encryption program receives adequate management oversight to timely address significant changes to the program. In addition, the IRS stated that it is exploring new technologies and technology enhancements and will implement a solution that will ensure that data at rest is encrypted prior to being transferred from the IRS to Private Collection Agencies.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 27, 2021

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement (Audit #202120008)

This report presents the results of our review to evaluate the implementation of the Internal Revenue Service's (IRS) Data at Rest Encryption Program. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

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

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, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

Data at rest encryption refers to the protection of data residing on system components (*i.e.*, data that are not in process or in transit) from unintended usage by applying encryption technology. Encryption solutions provide cryptographic protection (*i.e.*, making data unreadable to prevent anyone but approved individuals from reading that data) to the confidentiality and integrity of data in the event of unauthorized access or theft. Data at rest encryption is part of a comprehensive defense-in-depth strategy. The selection of applicable encryption solutions should be based on factors such as risk to the data, suitability of encryption options, as well as infrastructure capabilities.

The Data at Rest Encryption (DARE) program (hereafter referred to as the Program) was created in April 2018 to address the need for encryption to protect data across the Internal Revenue Service (IRS) enterprise. It is a multiyear, technical engineering effort charged with defining the architecture for enabling encryption at the storage, file system, database, and application levels for data center applications and systems.

The IRS relies extensively on computerized systems to support its financial and mission-related operations. In Fiscal Year 2020, the IRS collected close to $3.5 trillion in gross taxes and processed more than 240 million Federal tax returns and supplemental documents. The size and complexity of the IRS adds unique operational challenges. It must ensure that its computer systems are effectively secured to protect sensitive financial and taxpayer data and that they are operating as intended. In addition, successful modernization of IRS systems as well as the development and implementation of new information technology applications are necessary to meet evolving business needs. For a perspective on the challenges faced by the Program, it has identified more than [redacted] systems that require some type of data at rest encryption.

The Program addresses the need for protection of data at rest across the IRS.

A March 2018 internal IRS study[1] determined that a data at rest encryption strategy is feasible and can be effective even for a large agency with critical data and a varied infrastructure like the IRS. It also noted that while there is no one-size-fits-all answer to protect data at rest from an enterprise point of view, a centralized approach to development and adoption of data at rest encryption capabilities is recommended.

The IRS's April 2019 Integrated Modernization Business Plan, which outlines the major components necessary to modernize technology in support of the IRS mission over a six-year period, included two data at rest activities: to pilot its DARE implementation by June 2020 and to expand its DARE implementation by September 2020. The IRS also added to the plan an expectation to deploy a DARE Full Operating Capability[2] by September 2021 and to encrypt

[1] IRS, *Data at Rest Encryption Security Considerations* (March 8, 2018).

[2] Deploying a DARE Full Operating Capability refers to a specific set of requirements: end-to-end encryption integration with a key management solution and Oracle deployment to [redacted].

Treasury-designated High Value Assets (HVA)[3] by [redacted]. The HVAs are information technology assets that are deemed essential to an agency's ability to operate and execute its mission. These assets are mission-critical for the IRS to conduct tax administration functions and contain large amounts of sensitive information. Systems meeting these criteria have been identified across Federal Government agencies, and after being designated an HVA, the systems are subject to additional security and reporting requirements. For the Department of the Treasury, the HVAs can be identified by the Department or the bureau. The IRS has [redacted].

The June 2020 DARE Program Strategy document[4] defines the vision and goals. The strategic vision of the Program is that encryption of data at rest is applied to IRS mission-critical assets effectively and efficiently to reduce risk of data exposure while optimizing support of IRS business objectives. The Program has three goals:

- Identify and define a standardized set of data at rest encryption solutions for IRS enterprise system use in data center and cloud service environments.
- Assess the need for the acquisition of products and development for encryption and key management to efficiently enable DARE encryption solutions.
- Define and manage an implementation roadmap for deployment of DARE solutions, integrated with the program schedules of individual IRS enterprise information technology systems.

Key drivers of the Program strategy include ensuring compliance with encryption-related directives and guidance documents:

- National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Information Systems and Organizations* (Apr. 2013).[5]
- Office of Management and Budget Circular A-130 Revised, *Managing Information as a Strategic Resource* (July 2016).
- IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies* (Sept. 2016).
- Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (May 2019).
- Treasury Directive Publication 85-01, *Department of the Treasury Information Technology (IT) Security Program* (Sept. 2019).
- National Institute of Standards and Technology Special Publication 800-57 Part 1 Revision 5, *Recommendation for Key Management: Part 1-General* (May 2020).

[3] See Appendix III for glossary of terms.

[4] IRS, *Data at Rest Encryption (DARE) Program Strategy, Ver. 3.0* (June 10, 2020). Version 1.0 was created in April 2018.

[5] Version 4 of this Special Publication was the document used as a key driver for the Program strategy. The National Institute of Standards and Technology has since updated this Special Publication to Version 5, published in September 2020 and includes updates as of December 10, 2020.

In addition to these important directives and guidance documents, the IRS is required by law to protect tax-related information, such as tax returns and account information, and Personally Identifiable Information, which is information specific to a taxpayer, such as date of birth or mother's maiden name. The IRS must also protect proprietary organizational data that do not fall into these categories, including user account and system configuration information.

Another key driver of the Program is to address encryption-related recommendations from Treasury Inspector General for Tax Administration (TIGTA) and Government Accountability Office (GAO) audits. For example, TIGTA previously recommended that the IRS ensure that taxpayer data being transferred to Private Collection Agencies (PCA) are encrypted.[6] In addition, there have been several GAO recommendations to implement cryptographic mechanisms to secure taxpayer data in specific system environments.[7]

The Program strategy also emphasized the importance of having established enterprise-wide governance and processes in place in order to effectively plan and implement encryption and key management solutions.[8] The broad scope of the Program means most major information technology functions are stakeholders, and their active involvement is necessary to help ensure the success of the Program. These stakeholders include most Information Technology organization Associate Chief Information Officer functions, including Applications Development, Cybersecurity, Enterprise Operations, Enterprise Services, and User and Network Services. The Enterprise Services function is the primary coordinator of the DARE Program Strategy, and the responsible governance body is the Enterprise Services Governance Board, which is responsible for executive oversight of the Program, including the decision-making role to discuss program risks, issues, cost, scheduling, and scope variances and identify actions necessary to achieve desired results. It meets on a quarterly basis to monitor progress and address issues as they arise on programs and projects under its purview.

Results of Review

Given the amount of critical data maintained at the IRS and its diverse information technology infrastructure, the task of encrypting sensitive data across the entire IRS enterprise presents significant challenges. We determined that the IRS has made progress to identify and evaluate encryption and key management solutions for use with various groupings of systems with similar characteristics. However, it has yet to deploy any solutions. We also identified program issues that have affected the Program's progress towards meeting its goals to deploy a key management solution and encrypt systems in a production environment. In addition, we identified a prior encryption-related audit recommendation that was prematurely closed.

[6] TIGTA, Report No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

[7] GAO, GAO-20-411R, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls* (May 2020).

[8] A key management solution is used to manage encryption keys. This includes various activities, including key generation, exchange, distribution, rotation, replacement, storage, access, backup, and destruction. Encryption cannot be deployed without an associated working key management solution, also referred to as a key management system.

Progress Has Been Made to Identify and Test Encryption and Key Management Solutions

The Program developed a roadmap, which is a five-year plan (Fiscal Years 2019 through 2023) for establishing encryption solution standards and an enterprise key management solution. The roadmap included a framework to identify, classify, and group systems so that potential encryption solutions could be identified. We determined that the Program used this framework to identify system attributes, such as platform technology, programming language, and data format, and created natural groupings of systems, called technology clusters. As a result, these clusters could be potentially addressed by a single encryption solution. Examples of identified clusters include the Oracle® Database technology cluster and Linux® File System technology cluster.

The creation of technology clusters enabled identification and categorization of the diverse types of databases/platforms in use across the enterprise. The Program used the technology cluster information to identify potential encryption solutions by performing market research and identifying potential commercially available encryption and key management solutions for each cluster. Figure 1 shows the four primary groupings of systems requiring encryption identified by the Program, as well as the identified key management solutions and technology clusters that could utilize similar encryption agents.

Figure 1: DARE Key Management Solutions and Technology Clusters

Source: DARE Strategy Chief Information Officer Brief, March 9, 2021. COTS – Commercial-Off-The-Shelf, EKMF – Enterprise Key Management Foundation, AWS – Amazon Web Services.

The Program identified 15 technology clusters and related encryption and key management solutions to select systems for testing. It then conducted an Analysis of Alternatives to select a key management solution that was tested during the proof-of-concept process. Specifically, the Program tested the Oracle Transparent Data Encryption solution with integration to the Thales key management system proof-of-concept.

Encryption Plans Have Been Delayed

By the summer of Calendar Year 2020, the Program was in the process of planning for the Integrated Modernization Business Plan activity of deploying a DARE Full Operating Capability by September 30, 2021. To meet this commitment, the Program has to deploy an encryption solution and key management solution into a production environment, and then use them to successfully support [redacted].

However, in the summer of Calendar Year 2020, the Program was also tasked with a new priority to encrypt data on the HVAs along with the work already in progress to deploy the DARE Full Operating Capability. The requirement to encrypt the HVAs came from the Department of the Treasury as one of its initiatives to focus on cybersecurity across the Department. The IRS informed the Department of the Treasury that it would encrypt all HVAs by September 2026, and subsequently, the decision was made to encrypt the [redacted] Treasury-designated HVAs by [redacted].

The encryption of the HVAs was made a priority of the Program in the summer of 2020.

We identified specific program issues that have affected the ability of the Program to meet its goals. These include:

- Not following the Enterprise Life Cycle (ELC) requirements.
- Delays with developing an Integrated Master Schedule (IMS).
- Not prioritizing work related to prior encryption audit recommendations.

These issues have affected plans for HVA encryption as well as the progress with work related to deploying the DARE Full Operating Capability.

Successful programs have common elements, including the need for executive support as well as the existence of clear business objectives, methodologies, and project management expertise. Effective program governance is critical to the success of a program. Program managers depend on the governance board for continued organizational support for the program.

As mentioned previously, the Enterprise Services Governance Board is responsible for program governance and oversight of the DARE program. The Board's roles and responsibilities include managing a portfolio's performance and risk as well as Program decisions, risks, and issues. It generally has the authority to establish a program's baseline scope and schedule, and approve ELC milestone exits and risk and issue mitigations.

Program management is responsible for organizing and managing resources so that the Program's objectives are completed within defined scope, quality, time, and cost constraints. The Program's operations are assigned and managed by the Enterprise Services function but is comprised of personnel from various Information Technology functions as well as contractor personnel. Project management methodologies include the ELC framework, which establishes consistency and compliance with requirements for information technology programs.

In March 2021, the IRS moved this Program from the Enterprise Services function's Enterprise Architecture office to its Technology Strategy Management office to align the Program with the correct division. In addition, the IRS informed us that it conducted a top to bottom Program

review to address gaps and issues, including the ones we identified during the audit. This effort was ongoing as we completed our audit work.

The DARE Project did not follow ELC requirements

We determined that the DARE Project did not follow various ELC requirements, and this contributed to challenges faced by the Program. Specifically, Program management did not effectively utilize the ELC when they combined milestone exit reviews for multiple phases and did not timely update significant ELC artifacts.

The ELC is used to ensure consistency and compliance with government and industry best practices by information technology projects. It is the workflow that projects follow to move an information technology solution from concept to production while ensuring that the movement complies with IRS guidelines and the overall goals of the agency.

There are various ELC paths available for information technology projects, which are to be agreed upon at the start of new projects and documented in a Project Tailoring Plan. A path is an approach to accomplishing the life cycle work, and it specifies how work will be partitioned into phases. The Commercial-Off-the-Shelf path was chosen for the DARE Project, and it is comprised of phases that constitute broad segments of work that include similar activities and provide natural breakpoints in the life cycle. Figure 2 describes the phases, along with their related milestone numbers.

Figure 2: ELC Phases

Phase Name	Description	Milestone
Vision and Strategy/Enterprise Architecture	High-level direction setting.	MS 0
Project Initiation	Define project scope, form project teams, and begin many ELC artifacts.	MS 1
Domain Architecture	Gather, develop, and approve solution concept, requirements, and architecture.	MS 2
Preliminary Design	Development of Logical Design.	MS 3
Detail Design	Development of Physical Design.	MS 4a
System Development	Coding, integration, testing, and certification of solution/system.	MS 4b
System Deployment	Expand availability of solution to all target environments and users.	MS 5

Source: Internal Revenue Manual 2.16.1, Enterprise Life Cycle (July 10, 2017). MS – Milestone.

Milestones are important because they constitute a specific ending of one phase before moving to the next. Milestones are points at which management requires updated cost, progress, risk, and process information to make decisions regarding project funding and continuation. A project must complete a variety of required activities and have executive approval in order to exit each phase and move to the next.

Milestone exit requirements include the completion of various oversight review meetings as well as completed or updated required artifacts. Each phase concludes with a Milestone Readiness Review meeting, which is to review the project's progress, verify all exit requirements are met,

and make an executive recommendation as to whether the project is ready to exit the milestone. This process is to help ensure that projects do not advance to the next phase before the work on the current phase is complete; for example, the project does not start the design phase before the architecture phase is complete.

The DARE Project combined multiple ELC phases

As stated earlier, the Program is using the Commercial-Off-the-Shelf path, which is when pre-packaged, vendor-supplied software is to be used with little or no modification to provide all or part of a solution. This path has defined requirements; sequential progression through the phases, evolving teams, and uses a vendor solution for its technical approach. By using the tailoring process, changes can be made to the general ELC requirements to fit a specific project and are documented in the Project Tailoring Plan. The initial tailoring also determines what artifacts are required and at what point in the process.

While there are multiple sequential phases in this ELC path (as shown in Figure 2), it is common practice to combine the first two phases (Initiation and Architecture) with a single milestone exit for both. In addition, because it is based on using commercial software, both Design phases typically can be combined with a single milestone exit. However, during the tailoring process for the Program, it was agreed the Program would have a single milestone exit for Milestones 1 through 4a. This has the practical effect of deferring reviews of all of the milestone exit requirements until the project is at the end of the development phase. This could cause unnecessary delays if there were any adjustments or decisions about the design or scope of the project that needed to be addressed earlier. This also defeats the purpose of the ELC approach of having the project divided into phases with natural breakpoints, for which the project's progress can be reviewed periodically and necessary changes can be made.

We believe combining all four phases was not appropriate for the effective management of the Program. We discussed this issue with Program management and the ELC Office, which provides assistance to projects about how to follow the ELC process. Neither could provide a specific rationale as to why these phases were combined in this way. However, subsequent to our discussions, Program management and the ELC Office chose to revise this approach. An updated Project Tailoring Plan was issued in March 2021 requiring milestone exit reviews at Milestone 1/2 and Milestone 3/4a.

An example of the importance of having periodic milestone exits can be found in the required Business System Report artifact. The Business System Report serves as the primary reference for all project requirements for the project and is supposed to be completed and approved prior to exiting the Architecture phase (Milestone 2). Subsequent phases, such as Design (Milestones 3/4a), Development (Milestone 4b), and Deployment (Milestone 5), are based on the requirements and scope information in the approved Business System Report, so it is essential that it be completed and approved before exiting the Architecture phase. However, due to the ELC phases being combined, the DARE Business System Report was not completed or approved before development work was started. Correctly following the ELC process could have prevented this omission from happening.

Important ELC artifacts were not updated as required

We identified significant ELC artifacts that were not updated as required. For example, the Project Charter, Project Management Plan, and Project Tailoring Plan were not updated to

reflect the inclusion of HVA-related work in the project scope. Artifacts are used by a project to document how it plans to meet standards and requirements, and are usually in the form of documents based on pre-established templates. Both the Project Charter and Project Management Plan should have been reviewed and revised whenever the need for a significant project scope change became apparent, and should also have been reviewed and updated, if necessary, at the start of each ELC phase. In addition, a revision of the original Project Management Plan did not contain information related to the change in scope. Further, as previously mentioned, the DARE Business System Report was not completed and approved.

The Project Charter and Project Management Plan artifacts form the basis of project documentation and are some of the first artifacts to be prepared at the beginning of a project. The Project Charter provides the formal objectives, mandates, and scope for a project and specifies the business processes, key stakeholders, locations, requirements, systems, interfaces, tools, standards, and target releases addressed by the project.

The Project Management Plan describes the project's work and its approach to managing all project activities. The purpose of the Project Management Plan is to provide a framework for managing project activities and for completing the project successfully. The Project Tailoring Plan (discussed in prior section) is a documented agreement between the project manager and process owners regarding how the project will meet the established process requirements. It also identifies the artifacts and reviews required to be completed and any exceptions to the processes.

All of these artifacts were prepared in June and July 2020 when the project entered into the ELC process. However, they reflect the original project scope prior to HVA encryption-related work being prioritized. Program management did not ensure that these artifacts were updated to reflect the new scope of work related to HVA encryption, and this information was still not updated as of the end of April 2021. The Program officials stated that they understand the ELC process, but they had to keep moving forward with the work despite not meeting or completing specific requirements. However, we believe that proceeding to the development phase prior to completing the design or architecture phases could create confusion and uncertainty if the artifacts do not accurately reflect the current project scope, thus reducing their effectiveness and usefulness for project management and resulting in unnecessary delays.

Development of the IMS was delayed

The Program developed a DARE Program Management Framework document (April 2021) that provides guidance on various governance and program management activities, and includes background, instructions, templates, and samples for many of these activities. However, the Program did not follow its own guidance when developing the IMS. It took approximately eight months to create the initial IMS baseline (*i.e.*, approved version). While the schedule was being approved through the governance process, the project used the un-baselined schedule to track and manage program activities. The baseline IMS is meant to be the starting point from which all project activities are managed.

The DARE Program Management Framework separates the schedule process into three phases: development, baselining, and maintaining/updating the schedule. The first two phases focus on the approval of the IMS, so that the third phase can be carried out.

- The initial IMS is developed by leveraging several ELC artifacts and stakeholder working sessions. Upon ELC path approval, the Project Tailoring Plan and high-level timeline are referenced when building the IMS. Then, the scope definition process for the program will be used for planning and assumptions, and delivery partners will have meetings to identify and align on key milestone dates and reviews. The initial IMS is built from these working sessions.
- This initial IMS then goes through a baseline process. Key activities needed to complete the Program's work are captured, including inputs from Unified Work Requests and Program commitment dates. The DARE Program Office should propose durations for each task, with delivery partners reviewing them and providing feedback based on the ability to commit to these durations. Finally, a schedule walkthrough is conducted to validate activities and gain concurrence from delivery partners. After the walkthrough, the schedule is baselined. The baseline is the fixed project schedule used to measure program progress and contract performance, and when it is approved, the maintenance and updating phase begins.

In June 2020, the IRS entered into the ELC process when it started the development of the IMS based on the scope of the Program at that time. The baseline schedule was not initially approved until February 2021, and the IRS used various ad hoc methods to manage the Program until it was approved. In May 2021, Program management informed us that there were issues with gaps between dependencies and tasks that needed to be addressed, and that the IMS would have to be re-baselined. According to the IRS, IMS reviews and revisions were completed in June 2021, and the IMS was formally approved through the governance process on July 29, 2021.

Project management issues contributed to the IMS delays, including difficulties in obtaining timely, useful feedback from delivery partners as well as having to work with feedback comments based on various versions of the IMS. Based on the extended time taken for this process, we are concerned that the Program has been working on implementing an encryption solution at the same time as developing the related schedule that includes necessary information to effectively manage and measure the progress of the Program. Without a baseline IMS, the Program has no reliable schedule with which to gauge progress or to allocate resources. This increases the difficulty of effectively managing such a large project with multiple interdependencies and could further contribute to delays with meeting milestones or other deadlines.

Prior encryption recommendations were not prioritized and could impact the DARE Program's ability to meet deadlines

Prior to March 2021, the Program priorities were to deploy the DARE Full Operating Capability by September 30, 2021, and to encrypt Treasury-designated HVAs by [redacted]. However, in March 2021, the Program was also tasked with additional work unrelated to meeting those priorities. Specifically, the decision was made to include work to address prior GAO audit recommendations for encryption of certain systems. By not including this additional work earlier, the Program's ability to meet both the Full Operating Capability and Treasury-designated HVA encryption deadlines could be affected.

A GAO report [redacted][9] [redacted]. IRS management neither agreed nor disagreed with the recommendations, but stated that they would review each of the recommendations and ensure that corrective actions include sustainable fixes that implement appropriate security controls. The due date for the planned corrective actions was originally May 15, 2020, which was later extended to May 15, 2022. According to the IRS, initial DARE planning in Calendar Year 2018 for proof-of-concept testing specifically indicated that the focus should be on systems mentioned in the GAO report, and one system had proof-of-concept testing in November 2019. However, the work to address the planned corrective actions was not made a priority until March 2021.

Although the IRS prepared a briefing for the GAO about the Program's progress in March 2020, this briefing did not include information about addressing the GAO recommendations during Calendar Years 2020 or 2021. [redacted]. However, significant additional work is also needed to ensure that the encryption of the systems in question is accomplished timely. Prior to March 2021, that work was not included as a Program goal or in the IMS that was in the process of being baselined.

The Program's work on Full Operating Capability and Treasury-designated HVAs involves significant planning, testing, and procurement activities in order to meet the associated deadlines. In addition, other activities are in progress concurrently with those efforts, including creation of an IRS-designated HVA encryption implementation plan and the continuation of testing and development of technology cluster solutions. The Program was aware of the need to address the GAO recommendations as early as Calendar Year 2018, but did not make it a priority until March 2021, when the deadline for closing the corrective actions was approaching. The Program's governance oversight body is responsible for ensuring that the priorities are being addressed and for making necessary executive decisions to ensure the success of the Program.

The success of the Treasury-designated HVA encryption effort is partially dependent on the work to deploy the DARE Full Operating Capability, and encryption of some HVAs cannot be achieved without first successfully deploying the key management solution and Oracle encryption solutions. The notional schedule to address the GAO recommendations is very aggressive, and could directly impact the DARE Full Operating Capability deployment and HVA encryption plans. Therefore, delays with determining the priority of work related to the GAO recommendations could have significant negative impacts on these efforts.

The cause of these issues reported is that management did not effectively follow the ELC and provide sufficient oversight of the project, which allowed these conditions to exist. Unnecessary delays with deploying data at rest encryption, especially for HVA systems, will result in sensitive data for millions of taxpayers remaining at risk of exposure or theft.

[9] [redacted].

The Chief Information Officer should:

Recommendation 1: Ensure that the DARE program follows ELC requirements, including those for regular milestone exits prior to deployment to a production environment, and ensure that ELC artifacts are reviewed, updated, and approved as required.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Services, will ensure that the DARE program follows ELC requirements, including those for regular milestone exits prior to deployment to a production environment, and ensure that ELC artifacts are reviewed, updated, and approved as required.

Recommendation 2: Ensure that the DARE program follows the established process to develop and baseline the IMS, and verify the existing schedule information is accurate, including realistic time frames and task start and end dates.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Services, will ensure that the DARE Program Office follows the established process to create and baseline the IMS, and verify the existing schedule information is accurate, including realistic time frames and task start and end dates.

Recommendation 3: Ensure that the DARE program receives adequate management oversight, including following established processes, to timely address significant changes to the DARE program scope, risks, or constraints.

> **Management's Response:** The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Services, will ensure that the DARE program receives adequate management oversight, including following established processes, to timely address significant changes to the DARE program scope, risks, or constraints.

Corrective Action to Address a Previously Identified Encryption Security Weakness Was Not Fully Implemented

In July 2018, TIGTA reported[10] that end-to-end encryption was not enforced for the transferring of taxpayer data to and from the PCAs.[11] Specifically, TIGTA identified that taxpayer information used by the PCAs was not encrypted by either the IRS or the PCAs prior to being transferred. This information is supplied electronically to the PCAs so they can attempt the collection of tax debts, and the information about the amounts collected is then returned to

Corrective action to encrypt data at rest before transmission to the PCA was prematurely closed.

[10] TIGTA, Report No. 2018-20-039, *Private Collection Agency Security Over Taxpayer Data Needs Improvement* (July 2018).

[11] On December 4, 2015, the President signed into law the Fixing America's Surface Transportation Act, which included provisions amending Internal Revenue Code §§ 6306 and 6307 pertaining to the use of qualified tax collection contractors to collect inactive tax receivables. To address this legislative mandate, the IRS established a Private Debt Collection Program and selected four PCAs. The IRS enabled these designated contractors to collect outstanding inactive tax receivables on the Government's behalf.

the IRS. This taxpayer information is considered data at rest prior to being transferred, and is required to be encrypted by both the IRS and the PCAs. TIGTA recommended that the Chief Information Officer ensure that the data at rest be encrypted by the IRS and by the PCAs. In July 2019, the IRS closed this recommendation as completed.

Prior to closing the recommendation, the IRS verified the taxpayer information was being encrypted through e-mail verification with the PCAs. In addition, the IRS verified encryption of the PCAs' data through annual testing established by Publication 4812, *Contractor Security and Privacy Controls* (October 2019). Publication 4812 defines basic security and privacy control requirements and standards required of contractors (and contractor employees) when the contract involves access to, development, hosting, or maintenance of Sensitive but Unclassified information. Sensitive but Unclassified data include Federal tax information (*i.e.*, taxpayer information) and Personally Identifiable Information. Based on this testing, the IRS determined that the PCAs were encrypting the taxpayer information as required.

In addition, the IRS completed a feasibility study to determine how it could implement data at rest encryption for taxpayer information prior to it being transferred to the PCAs. This feasibility study concluded that IRS-based options would require further testing to ensure compatibility. It also concluded that access to necessary resources would need to be obtained to develop and implement any strategy for the encryption of taxpayer data prior to being transferred to the PCAs. Based on the feasibility study, the IRS conducted a pilot and determined that it was able to encrypt the data in both the Development and Test environments. Based on the results of the pilot, the IRS indicated it was planning to encrypt PCA information after it had completed encrypting two other systems. The IRS also stated that the encryption of data was resolved; however, we determined that PCA information residing at the IRS had not been encrypted in the production environment.

Internal Revenue Manual 1.4.30, *Resource Guide for Managers, Monitoring Internal Control Planned Corrective Actions* (October 2015), provides that it is the IRS's responsibility to ensure that recommendations are implemented. In addition, the heads of all business units are required to certify that the corrective actions they are responsible for were met. Furthermore, Treasury Directive Publication 40-03, *Treasury Audit Resolution, Follow-up, and Closure* (May 2017), states that the IRS is responsible for ensuring that all recommendations are appropriately addressed and corrective actions are well-defined, address and resolve the root causes and impact of the problem, are taken in a timely fashion, and are verified through independent verification. Until data at rest encryption is employed for these sensitive data, which include Federal tax information and Personally Identifiable Information, it will remain at risk of exposure or unauthorized access.

Recommendation 4: The Chief Information Officer should ensure that data at rest is encrypted prior to being transferred from the IRS to the PCAs.

Management's Response: The IRS agreed with this recommendation. The Associate Chief Information Officer, Enterprise Services, is exploring new technologies and technology enhancements, and will implement a solution that will ensure that data at rest is encrypted prior to being transferred from the IRS to the PCAs.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the implementation of the DARE program. To accomplish our objective, we:

- Evaluated DARE program implementation plans to determine if they are reasonable and will enable the IRS to encrypt data at rest on all relevant IRS systems to include Treasury-designated IRS HVAs and IRS-designated HVAs.
- Evaluated program documentation and interviewed key personnel to determine the progress made by the DARE program to identify, evaluate, and test commercial key management and encryption solutions.
- Evaluated program documentation and interviewed key personnel to determine whether the DARE program properly followed ELC requirements and prepared artifacts as required.
- Evaluated versions of the program IMS and other planning tools to determine if they are adequate and realistic.
- Reviewed prior audit reports and program documentation to identify previously reported data at rest encryption issues and determine if the issues were effectively resolved.

Performance of This Review

This review was performed with information obtained from the Enterprise Services function located in the New Carrollton Federal Building in Lanham, Maryland, during the period November 2020 through July 2021. 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Kent Sagara, Director; Joseph Cooney, Audit Manager; Steven Stephens, Lead Auditor; and Midori Ohno, Senior Auditor.

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 sections 2.16.1, *Enterprise Life Cycle* (Nov. 2019); 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (May 2019); and 1.4.30, *Resources Guide of Managers Monitoring Internal Control Planned Corrective Actions* (Oct. 2015); Treasury Directive Publication 40-03, *Treasury*

Audit Resolution, Follow-Up, and Closure (May 2017); and National Institute for Standards and Technology Special Publications 800-53 Revision 4 *Security and Privacy Controls for Information Systems and Organizations* (Apr. 2013) and 800-57 Part 1 Revision 5, *Recommendation for Key Management: Part 1-General* (May 2020), for requirements for protection of information at rest. We evaluated these controls by interviewing the DARE program team and ELC organization personnel, as well as reviewing relevant documentation pertaining to various program activities.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

September 17, 2021

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer

Kaschit D. Pandya

Digitally signed by Kaschit D. Pandya
Date: 2021.09.17 12:01:42 -04'00'

SUBJECT: Response to Draft Audit Report – The Data at Rest Encryption Program Has Made Progress With Identifying Encryption (e-trak # 2021-40004).

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. The Data At Rest Encryption (DARE) effort at the IRS is an enormous undertaking with far reaching impact on programs and taxpayers. The IRS has already identified solutions for our open systems and IBM Mainframe environment and is on track to complete our modernization plan objective of having Full Operational Capability (FOC) for Oracle encryption by December 15th. Additionally, the IRS is on track complete encryption to remediate and close the Planned Corrective Actions (PCA) for Oracle applications findings from previous GAO Audits by August 31, 2022.

These complex undertakings, which are occurring concurrently with the delivery of filing season, require teams across the IRS to coordinate and decipher complex requirements and identify impact on tax processing systems. The IRS has made significant progress toward executing the plan for our Oracle database systems. The Key Management System (KMS) is already operational in our non-production environments where the applications selected for the FOC have been encrypted as well. Once operational in production in December, the KMS will allow IRS to Encrypt a large portion of our High Value Assets (HVA). In parallel, the IRS is working with strategic partners to implement the Key Management capability for our Mainframes, enabling IRS to encrypt the remaining High Value Assets well in advance of Treasury's 2026 requirement.

We agree with TIGTA's four recommendations and will continue to ensure that governance and oversight are followed in accordance with the IRM and ELC processes. Our corrective action plan for the recommendations identified in the report is attached. The IRS is committed to meeting the needs of the American people to implement and maintain a safe and secure environment.

The IRS values TIGTA's continued support and assistance. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Marci Weiskott, Director, Technology Strategy Management, at (301) 452-8056.

Attachment

RECOMMENDATION 1
The Chief Information Officer should ensure that the DARE program follows the ELC requirements, including those for regular milestone exits prior to deployment to a production environment, and ensure that ELC artifacts are reviewed, updated, and approved as required.

CORRECTIVE ACTION 1
The IRS agrees with this recommendation. The ACIO, Enterprise Services will ensure that the DARE program follows the ELC requirements, including those for regular milestone exits prior to deployment to a production environment, and ensure that ELC artifacts are reviewed, updated, and approved as required.

IMPLEMENTATION DATE
August 15, 2022

RESPONSIBLE OFFICIAL(S)
ACIO, Enterprise Services

CORRECTIVE ACTION Monitoring Plan
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 2
The Chief Information Officer should ensure that the DARE program follows the established process to create and baseline the Integrated Master Schedule, and verify the existing schedule information is accurate, including realistic timeframes and task start and end dates.

CORRECTIVE ACTION 2
The IRS agrees with this recommendation. The ACIO, Enterprise Services will ensure that the DARE Program Office follows the established process to create and baseline the Integrated Master Schedule, and verify the existing schedule information is accurate, including realistic timeframes and task start and end dates.

IMPLEMENTATION DATE
August 15, 2022

RESPONSIBLE OFFICIAL(S)
ACIO, Enterprise Services

CORRECTIVE ACTION Monitoring Plan
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 3
The Chief Information Officer should ensure the DARE program receives adequate management oversight, including following established processes, to timely address significant changes to the DARE program scope, risks, or constraints.

CORRECTIVE ACTION 3
The IRS agrees with this recommendation. The ACIO, Enterprise Services will ensure the DARE program receives adequate management oversight, including following established processes, to timely address significant changes to the DARE program scope, risks, or constraints.

IMPLEMENTATION DATE
August 15, 2022

RESPONSIBLE OFFICIAL(S)
ACIO, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN
IRS will monitor this corrective action as part of our internal management system of controls.

RECOMMENDATION 4
The Chief Information Officer should follow the Internal Revenue Manual and Treasury Directive guidance and ensure that the prior recommendation to encrypt taxpayer data at rest for Private Collection Agencies is appropriately addressed. This includes reopening and monitoring the closed recommendation to ensure data at rest is encrypted prior to being transferred from the IRS to Private Collection Agencies.

CORRECTIVE ACTION 4
The IRS agrees with this recommendation. The ACIO, Enterprise Services is exploring new technologies and technology enhancements and will implement a solution that will ensure data at rest is encrypted prior to being transferred from the IRS to Private Collection Agencies.

IMPLEMENTATION DATE
August 15, 2023

RESPONSIBLE OFFICIAL(S)
ACIO, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN

IRS will monitor this corrective action as part of our internal management system of controls. This includes reopening the new PCA and monitoring the closed recommendation to ensure data at rest is encrypted prior to being transferred from the IRS to Private Collection Agencies.

Appendix III

Glossary of Terms

Term	Definition
Analysis of Alternatives	An analytical comparison or evaluation of proposed approaches to meet an objective. The formal or informal process involves identifying key decision factors, such as life cycle operations, support, training, and sustaining costs; risks; effectiveness; and assessing each alternative with respect to these factors.
Artifact	The output of an activity performed in a process/procedure, which is created throughout the life cycle of a project.
Delivery Partners	Organizations or individuals assigned responsibility and accountability for management of an enterprise process.
Detail Design Phase	Involves the development of an application's physical design and relates to how data are entered into a system, verified, processed, and displayed as output.
Domain Architecture Phase	Involves the development of a business system concept, business system requirements, and business system architecture.
Enterprise Life Cycle	A structured business systems development methodology that requires the preparation of specific work products during different phases of the development process. The ELC establishes a set of repeatable processes and system of reviews, checkpoints, and milestones that reduce the risks of system development and ensure alignment with the overall business strategy.
High Value Asset	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations or house unique collections of data (by size or content), making them of particular interest to criminal, politically motivated, or State-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the Government.
Integrated Master Schedule	Contains a high-level overview of project schedules along with additional program tasks, including high-level start/end dates, project/application milestones, cross-project dependencies, and program milestones.
Milestone	A management decision point placed at a natural breakpoint in the life cycle, at the end of the phase, where management determines whether a project can proceed to the next phase.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, and biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth and mother's maiden name.

Term	Definition
Preliminary Design Phase	Involves developing the application's logical design. Logical design pertains to an abstract representation of the data flow, inputs, and outputs of the system.
System Deployment Phase	Involves expanding the availability of the solution to all target environments and users. It results in transferring support to an organization other than the developers and signifies the end of project development.
System Development Phase	Involves coding, integrating, and testing the application. It results in the authorization to put the solution into production.

Appendix IV

Abbreviations

DARE	Data at Rest Encryption
ELC	Enterprise Life Cycle
GAO	Government Accountability Office
HVA	High Value Asset
IMS	Integrated Master Schedule
IRS	Internal Revenue Service
PCA	Private Collection Agency
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

Information you provide is confidential, and you may remain anonymous.