TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Network Segmentation Reduced Unnecessary Access to Individual Master File Resources; However, Governance and Development Processes Were Not Always Followed

February 2, 2022

Report Number: 2022-20-010

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

HIGHLIGHTS: Network Segmentation Reduced Unnecessary Access to Individual Master File Resources; However, Governance and Development Processes Were Not Always Followed

Final Audit Report issued on February 2, 2022 **Report Number 2022-20-010**

Why TIGTA Did This Audit

The IRS's Network Segmentation Project was implemented as a solution that would allow users to navigate only to authorized resources within its internal network and initiate cybersecurity alerts when unauthorized users and devices attempt to connect to the internal network to access resources.

This audit was initiated to evaluate the effectiveness of Information Technology organization efforts to limit the internal network risk exposure by segmenting key information technology systems.

Impact on Taxpayers

The IRS has made implementing network segmentation for designated High Value Assets a priority. A High Value Asset is defined as an information system, information, or data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the economy or public confidence.

The Department of the Treasury has identified six IRS systems that contain taxpayer data as High Value Assets. Implementing network segmentation for these six systems will allow the IRS to implement secure network access to taxpayer data through user and device authentication as well as user and device authorization.

What TIGTA Found

The IRS installed, configured, and enabled Cisco's Identity Services Engine and TrustSec products to implement a solution that would allow users to navigate only to authorized resources within the internal network. In September 2020, the User and Network Services function deployed network segmentation for the Individual Master File (IMF).

Deploying network segmentation for the IMF reduced the number of users who had access to the mainframe logical partitions where the IMF runs from [redacted], eliminating the unnecessary access of a significant number of users. The [redacted], that run on the same mainframe logical partitions as the IMF.

The IRS refers to its development process as the Enterprise Life Cycle (ELC) framework, which is comprised of various phases. At the end of each phase, a Milestone Exit Review is required, during which management reviews updated cost, progress, risk, and process information to decide if the project should continue. However, the User and Network Services Governance Board did not complete the mandatory Milestone Exit Reviews for the IMF network segmentation project. This board also had the authority to approve the IMF network segmentation project's migration to production; however, the board's approval was not obtained prior to deployment. Further, key development artifacts for the IMF network segmentation project were not completed or lacked critical content.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that: 1) ELC framework artifacts are completed and Milestone Exit Reviews are conducted by network segmentation projects prior to deployment to production; 2) project teams obtain governance board approvals prior to deploying development project solutions to production; 3) the *Simplified Design Specification Report* for network segmentation is updated to describe the complexity of the design and the limits of the Identity Services Engine and TrustSec products; and 4) a *System Test Plan* is developed and executed for network segmentation to include test cases for key requirements, test results, and test case resolution for failed tests.

The IRS agreed with two recommendations. The IRS plans to complete the required artifacts for future network segmentation efforts and revise the *System Test Plan*. The IRS disagreed that project teams obtain governance board approvals prior to deploying development project solutions to production. The IRS states that senior leadership approval may come prior to governance approval. Governance is a key control over the implementation of the ELC process and solution development. Senior leadership approval should not be used to circumvent the role of the governance board.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

February 2, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Network Segmentation Reduced Unnecessary Access to Individual Master File Resources; However, Governance and Development Processes Were Not Always Followed (Audit # 202120014)

This report presents the results of our review to evaluate the effectiveness of Information Technology organization efforts to limit the internal network risk exposure by segmenting key information technology systems. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] 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

In Calendar Year 2012, the Internal Revenue Service (IRS) conducted penetration testing[1] that disclosed significant security vulnerabilities in its internal local area network. These vulnerabilities indicated that the internal network environment was not secure and raised the possibility of undetected accesses to sensitive taxpayer data. As a result, the Information Technology (IT) organization initiated the Unified Access Project and later the Network Segmentation (SEG) Project, hereafter referred to as the SEG Project, to resolve these vulnerabilities. The goal of the Unified Access Project was to authenticate users and devices regardless of connection type, *i.e.*, through wired, wireless, or virtual private network connections. Specifically, it was to ensure that only valid users and devices were permitted access to the IRS's internal network. The purpose of the SEG Project was to implement a solution that would allow users to navigate only to authorized resources within the internal network and initiate cybersecurity alerts when unauthorized users and devices attempt to connect to the internal network or access resources. The IT organization's User and Network Services (UNS) function managed the development and deployment of both projects.

The IRS has made implementing network segmentation for designated High Value Assets (HVA) a priority. An HVA is defined as an information system, information, or data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the economy or public confidence. The Department of the Treasury has identified six IRS systems that contain taxpayer data as HVAs. These include the:

1) [redacted].
2) [redacted].
3) Individual Master File (IMF) – A system that receives individual tax submissions in an electronic format and produces refund data, notice data, reports, and information feeds to other IRS entities.
4) Integrated Data Retrieval System – A system capable of retrieving or updating stored information in a taxpayer's account records.
5) [redacted].
6) [redacted].

[1] See Appendix III for a glossary of terms.

In September 2020, the UNS function deployed network segmentation for the IMF. In July 2021, the UNS function deployed network segmentation for [redacted], the Integrated Data Retrieval System, and [redacted]. The UNS function plans to deploy network segmentation for the remaining HVA, [redacted], in the future. Implementing network segmentation for its six HVAs will allow the IRS to implement secure network access to taxpayer data through user and device authentication as well as user and device authorization.

To implement unified access and network segmentation, the UNS function installed, configured, and enabled Cisco's Identity Services Engine and TrustSec® products, which are commercial off-the-shelf software. The Identity Services Engine evaluates each user's and device's credentials to determine if they are valid. If valid, the Identity Services Engine authenticates their identities. Authentication is the process of verifying the identity of a user or device. To segment authenticated users and devices, TrustSec relies on authorization through the Identity Services Engine. Authorization is the act of granting access privileges to a user, program, or process. The integration of the Identity Services Engine and TrustSec products allows for secure network access through user and device authentication as well as user and device authorization to authorized network resources.

Network segmentation was implemented for users connecting to the IRS's internal local area network through wired, wireless, and virtual private network connections. Two sequential modes, audit and secure, were completed to implement network segmentation. Audit mode allowed the SEG Project Team to see all users and what resources they were accessing. When the SEG Project Team subsequently implemented secure mode, only properly authorized users could access network resources controlled by the Identity Services Engine and TrustSec products. TrustSec involves the following three phases: classification, propagation, and enforcement.

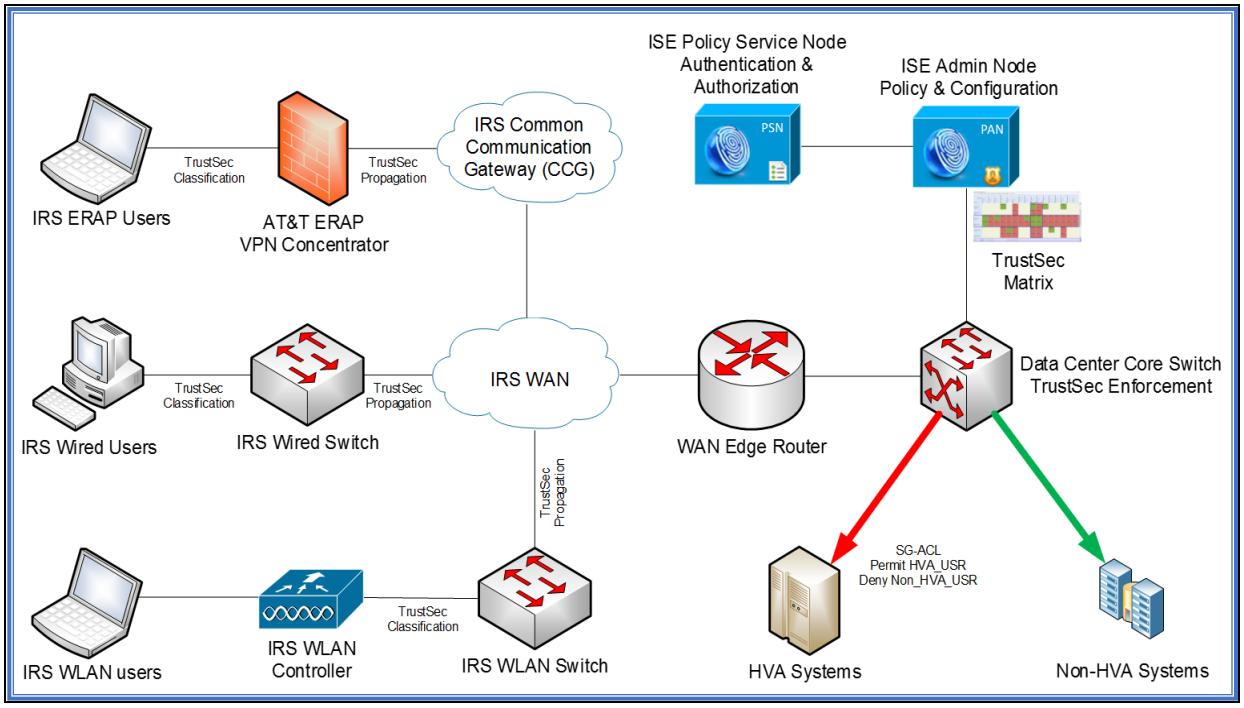
Classification

During the classification phase, a user is authenticated, authorized, and assigned a Security Group Tag. A Security Group Tag is defined by a user Security Group Name and a number between 1 and 65,535. Security Group Tags allow TrustSec to create policies based on a user, device, or server's role in the network as compared to Internet Protocol addresses in a Security Group Access Control List. Security Group Tags are also assigned to resources, such as servers and mainframe logical partitions.

Propagation

After Security Group Tags are assigned or classified to users and resources, they are propagated across the internal network to network access devices, such as wired and wireless switches, until they reach the Wide Area Network edge routers to be grouped and forwarded to the data center core switches for enforcement. Figure 1 is a graphic that shows the IRS's network segmentation infrastructure.

Figure 1: Network Segmentation Infrastructure

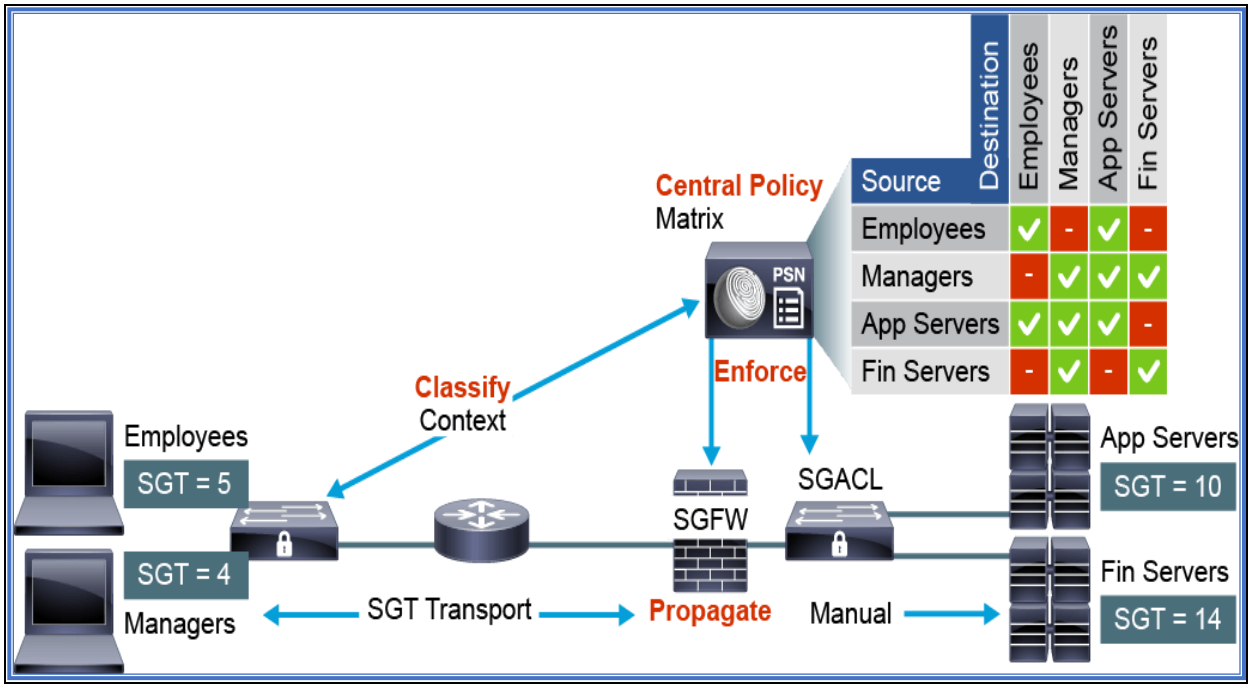


Source: UNS function's Network Engineering personnel as of June 3, 2021. Admin – Administration; ERAP – Enterprise Remote Access Program; ISE – Identity Services Engine; SG-ACL – Security Group–Access Control List; USR – User; VPN – Virtual Private Network; WAN – Wide Area Network; and WLAN – Wireless Local Area Network.

Enforcement

Enforcement is the process by which a TrustSec policy is acted upon to control access. Enforcement is carried out using a Security Group Access Control List, which provides a more detailed level of access control to resources. Enforcement of Security Group Access Control List policies within TrustSec is implemented by a TrustSec permissions matrix, with source Security Group Tags on one axis and destination Security Group Tags on the other axis. Each cell in the body of the matrix can contain a Security Group Access Control List. The TrustSec matrix and the associated Security Group Access Control List are downloaded to the enforcement devices, which are two data center core switches. Using a Security Group Access Control List, the IRS can control the operations that users can perform based on the security group assignments of users and destination resources. Figure 2 illustrates the TrustSec's three phases, *i.e.*, classification, propagation, and enforcement, as related to Security Group Tags.

Figure 2: TrustSec Classification, Propagation, and Enforcement of the Security Group Tags



Source: Cisco Identity Services Engine Student Guide, dated September 2020. App Servers – Application Servers; Fin Servers – Financial Servers; PSN – Policy Service Node; SGACL – Security Group Access Control List; SGFW – Security Group Firewall; and SGT – Security Group Tag.

The enforcement phase is universal to all three connection types, *i.e.*, wired, wireless, and virtual private network. The same data center core switches are the common enforcement mechanisms used to determine whether wired, wireless, and virtual private network traffic destined to HVA systems is allowed or denied.

Results of Review

Network Segmentation Reduced the Number of Users Potentially Able to Access Individual Master File Resources

The IMF runs on an International Business Machines® (IBM) Corporation mainframe computer located at the IRS's Enterprise Computing Center in Martinsburg, West Virginia. The Identity Services Engine and TrustSec products implement access controls over network resources by using Security Group Tags tied to Internet Protocol addresses. There is only one TrustSec Security Group for all IMF users. This group identifies the users allowed access to IMF resources. IMF resources are allocated to five logical partitions on the mainframe and the logical partitions are identified by their Internet Protocol addresses. However, TrustSec is able to control access to only the mainframe logical partition level. Thereafter, to access specific IMF resources that are allocated to the logical partitions, the Identity Services Engine and TrustSec products pass access enforcement to IBM's Resource Access Control Facility. The Resource Access Control Facility product manages the authentication and authorization controls to enforce access to the IMF file-level resources.

According to an *IRS Progress Update Fiscal Year 2020 Report*,[2] prior to deploying network segmentation for the IMF, [redacted] were able to reach the mainframe logical partitions where the IMF runs. After network segmentation was deployed for the IMF, the number of users able to reach IMF-related partitions was reduced to [redacted] eliminating the unnecessary access of a significant number of users. The [redacted], that run on the same mainframe logical partitions as the IMF.

Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy, and Guidance*,[3] lays the foundation to implement and manage information system security within the IRS. Specifically, Internal Revenue Manual 10.8.1.4.1.1, *AC-2 Account Management*, states that authorized access to an information system should be based on valid access authorization and intended system usage.

For users to obtain authorization to access IMF resources, they must complete an Online 5081 request. Once the Online 5081 request is approved, the user is assigned to an IMF-related Online 5081 user security group. Based on the Online 5081 user security groups, the IRS created [redacted] that are used to authenticate users through the Identity Services Engine.

To test the access and authorization controls, we obtained audit logs from December 1, 2020, showing 1,441 audit log records and selected a judgmental sample[4] of 30 of the 75 users who accessed IMF resources during a four-hour period. We verified that all 30 users were properly authorized to access the IMF resources. Further, we reviewed configuration settings and the results of Identity Services Engine and TrustSec queries and validated that the classification, propagation, and enforcement phases of network segmentation were enabled. We also determined that the Identity Services Engine authorization policies were reasonable and complete; therefore, network segmentation was enabled to deploy IMF access and authorization controls.

Insufficient Management Oversight Allowed the Network Segmentation Project to Bypass Mandated Governance and Development Processes

The IRS refers to its development process as the Enterprise Life Cycle (ELC) framework. The ELC framework is the workflow that projects follow to move an information technology solution from concept to production. The ELC framework includes phases, and each phase constitutes broad segments of work that encompass activities of similar scope, nature, and detail, and provides for a natural breakpoint in the project life cycle. At the end of each phase, a Milestone Exit Review is required. The ELC framework phases are:

1) The Project Initiation phase (Milestone 1) defines the project scope, forms the project team, and begins development of the ELC framework artifacts.
2) The Domain Architecture phase (Milestone 2) develops the concept solution, requirements, and architecture.

[2] Dated December 2020.

[3] Dated May 2019.

[4] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

3) The Preliminary and Detailed Design phases (Milestones 3 and 4a) develop the logical and physical design.

4) The System Development phase (Milestone 4b) completes the integration, testing, and security certification. The completion of this phase results in the authorization to migrate the development solution to production.

5) The System Deployment phase (Milestone 5) expands the solution to all target environments and users.

In April 2020, the SEG Project Manager signed the *SEG Project Tailoring Plan* agreeing that the SEG Project would follow the ELC framework's commercial off-the-shelf development path. The IRS uses this development path when prepackaged, vendor-supplied software is used with little or no modification to provide all or part of the development solution. At that time, the SEG Project Team did not believe that sufficient time was available to complete the ELC framework phases and related artifacts by June 30, 2020, *i.e.*, the initial completion date for deploying network segmentation for the IMF. As a result, UNS function management proposed combining ELC framework Milestones 1 through 4a,[5] and the ELC office approved the process change. Shortly thereafter, UNS function management approved completing the ELC framework and deploying network segmentation for IMF to production by September 30, 2020. In September 2020, the UNS function's Director, Network Engineering, approved the release of the SEG Project to production. At that time, some of the mandatory ELC framework processes and artifacts were not completed, including:

1) The *Simplified Design Specification Report* was not completed prior to the SEG Project's release to production and was not approved until December 2020. According to Internal Revenue Manual 2.16.1, *Enterprise Life Cycle*,[6] the *Simplified Design Specification Report* is an artifact that the project team is required to complete during development. It is the primary document to record a project's software design solution. The lack of an approved *Simplified Design Specification Report* during development could negatively affect the outcome of the project.

2) The UNS Governance Board[7] had not completed, and subsequently did not complete, any of the required Milestone Exit Reviews. From October 2018 through deployment in September 2020, the board held only two meetings in which the SEG Project Team presented the project's status. According to the IRS, these oversight reviews were not held because the Associate Chief Information Officer, UNS, and the SEG Project's Executive Sponsor were briefed and received communications via Associate Chief Information Officer briefings and monthly SEG Project Team meetings. However, the UNS Governance Board has several other executive and senior manager members that were apparently not briefed and did not fulfill their oversight responsibilities.

[5] ELC framework milestones are normally completed sequentially, with the next milestone beginning after the previous Milestone Exit Review has been completed.

[6] Dated November 2019.

[7] Members of the UNS Governance Board include the Deputy Associate Chief Information Officer, UNS; the Director, Contact Center Support; the Director, Customer Service Support; the Director, Enterprise Field Operations; the Director, Network Engineering; the Director, Operations Service Support; the Director, Service Planning and Improvement; and the Director, Unified Communications.

Nevertheless, the ELC framework still requires Milestone Exit Reviews. Internal Revenue Manual 2.16.1 identifies the phases of a development project, defines the artifacts that are required during each phase, and explains that each phase terminates at a milestone. Milestone Exit Reviews are mandatory reviews conducted by the assigned Governance Board in which management reviews updated cost, progress, risk, and process information to decide if the project should continue. The outcome of a Milestone Exit Review is a go/no-go decision that documents an unconditional approval, conditional approval, disapproval, or recommendation to suspend or to terminate the project. According to the *UNS Governance Board Charter*,[8] the board will direct adherence to the ELC framework and approve Milestone Exit Reviews. In addition, the *SEG Project Management Plan*[9] states that the SEG Project Team would hold quarterly status meetings with the board and would obtain board approval for Milestone Exit Reviews.

3) The UNS Governance Board had not approved the decision to release network segmentation for the IMF to production; in fact, the board's approval was not obtained prior to deployment. According to the *UNS Governance Board Charter*, the board will approve release launches to production. Therefore, the Director, Network Engineering, did not have the sole authority to deploy the network segmentation for the IMF to production. Further, without obtaining the board's approval prior to deploying the project solution, the SEG Project Team bypassed an agreed-upon information technology governance process.

   The IRS maintains that the necessary sponsor and stakeholder approvals were obtained prior to deploying network segmentation for the IMF to production in September 2020. Network Engineering personnel provided documentation that: 1) the Director, Network Engineering, discussed authorizing network segmentation to go live with the Associate Chief Information Officer, UNS, prior to deployment; 2) seven of the nine UNS Governance Board members were briefed on this initiative and its timeline during the Cybersecurity/UNS Monthly Meeting in January 2020; and 3) eight of the nine UNS Governance Board members were briefed in the UNS Quarterly Operations Review in December 2020. However, none of these actions equate to obtaining the UNS Governance Board's approval immediately prior to the deployment of the solution.

   In May 2018, to implement the Federal Information Technology Acquisition Reform Act of 2014,[10] the IT organization reorganized its governance structure. Further, to comply with the Taxpayer First Act of 2019,[11] the Chief Information Officer was given responsibility for overseeing the development, implementation, and maintenance of the IRS's information technology enterprise-wide through oversight provided by various information technology governance boards, including boards over Associate Chief Information Officer areas of responsibility, like the UNS Governance Board. Therefore, to implement information technology governance, board members needed to carry out

[8] Dated October 2020.

[9] Dated April 2020.

[10] Pub. L. No. 113-291, Title VIII, Subtitle D, 128 Stat. 3449, §§ 831-837 (codified as amended in 40 U.S.C. §§ 11302 and 11319; 41 U.S.C. § 1704 note; 41 U.S.C. § 3301 note; and 44 U.S.C. § 3601 note). Note: The Federal Information Technology Acquisition Reform Act is located in Title VIII, Subtitle D, of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, 128 Stat. 3449.

[11] Pub. L. No. 116-25, 133 Stat. 981 (codified in scattered sections of 26 U.S.C.).

their assigned duties; in this case, this means reviewing and approving the network segmentation release launches to production.

The lack of an approved *Simplified Design Specification Report* during development, the lack of Milestone Exit Reviews, and the lack of compliance with IT organization governance requirements regarding authority to launch releases to production are indicators of insufficient management oversight.

The Chief Information Officer should ensure that:

Recommendation 1: ELC framework artifacts are completed and Milestone Exit Reviews are conducted by network segmentation projects prior to deployment to production.

Management's Response: The IRS agreed with this recommendation. The IRS will complete the required ELC artifacts for future network segmentation efforts deemed as a project prior to deployment into production.

Recommendation 2: Project teams obtain governance board approvals prior to deploying development project solutions to production.

Management's Response: The IRS disagreed with this recommendation. Governance process is established and followed for delivering project solutions; however, senior leadership approval may often come prior to governance approval. Governance and artifacts are then updated and finalized.

Office of Audit Comment: Governance is a key control over the implementation of the ELC process and solution development. The SEG Project Team did not follow the governance process because no required Milestone Exit Reviews were conducted and the UNS Governance Board did not approve the release launch to production per its Charter. While it is important to obtain senior leadership approval, it should not be used to circumvent the role of the governance board. In addition, briefing board members on the project status is not a substitute for UNS Governance Board approval.

Key Development Artifacts Were Not Completed or Lacked Critical Content

According to the ELC framework, the *Simplified Design Specification Report* and the *System Test Plan* are required documents that are to be developed during the development process.

Simplified Design Specification Report

When the SEG Project Team deployed network segmentation for the IMF in secure mode, only properly authorized users could access IMF resources within the control of the Identity Services Engine and TrustSec products. Deploying network segmentation for the IMF was a complex undertaking as it involved hundreds of Online 5081 user security groups, thousands of users, and an unknown number of systems' file-level resources. According to Internal Revenue Manual 2.16.1, the *Simplified Design Specification Report* is the required document to record a project's software design solution. However, while the SEG Project's *Simplified Design Specification Report* was eventually approved in December 2020, it does not describe the complexity of the design nor the limits of the design to segment IMF users from non-IMF users.

In addition, the *Simplified Design Specification Report* does not describe the relationship between Cisco's Identity Services Engine and TrustSec products and the IBM Resource Access Control Facility. Further, the *Simplified Design Specification Report* does not mention the IMF-specific Online 5081 user security groups or system resources that are involved to deploy network segmentation for the IMF.

According to the IRS, the IMF and other HVA details were not included in the *Simplified Design Specification Report* because the SEG Project was not specifically directed at HVAs when the document was created in Calendar Year 2018. As a result of the IRS not updating the *Simplified Design Specification Report* to reflect the SEG Project's current HVA focus, it is not complete or relevant because critical design details related to the HVAs are not included.

System Test Plan

A *System Test Plan* summarizes the complete test effort for the information system release. When we asked the SEG Project Team to provide us with the SEG Project's *System Test Plan*, they provided a *System Test Plan* with identical testing content as the Unified Access Project's *System Test Plan;*[12] no additional testing was documented after the Unified Access Project testing was completed in September 2019. In a follow-up discussion, the SEG Project Manager clarified that additional monthly testing was conducted from June through September 2020, but the tests and results were not documented. This statement is consistent with seven e-mails that were subsequently provided, dated prior to deployment, which identified various actions that Network Engineering personnel completed. The e-mails included bulleted high-level statements using verbs like verified, confirmed, tested, and reviewed. However, the e-mail documentation was not requirements-driven and did not clearly identify:

1) The test objectives.
2) The requirements being tested.
3) The expected test results.
4) The actual test results.

Therefore, the documentation was insufficient for an independent reviewer to be able to analyze the results and conclude that key SEG Project requirements were adequately tested.

According to Internal Revenue Manual 2.16.1, the ELC framework's System Development phase completes the integration, testing, and security certification processes. In addition, Internal Revenue Manual 2.127.1, *Testing Standards and Procedures, Information Technology Test Policy*,[13] establishes standards, expectations, authority, and documentation responsibility for the development and facilitation of information technology testing standards.[14] This guidance applies to all testing[15] within the IT organization and specifies that all test plans must include strategies to verify system integration, acceptance, privacy, and security testing requirements.

[12] Dated September 2020.

[13] Dated May 2017.

[14] The Enterprise Services function's Enterprise Systems Testing is the owner of the testing process and testing standards.

[15] Includes testing of software applications, hardware, infrastructure projects, and new and legacy production system upgrade projects.

Lastly, all test artifacts, including plans, scripts, cases, reports, and measurements, must be recorded and maintained in an approved test repository.

Based on an interview with UNS function management, the Director, Network Engineering, who is the SEG Project's Executive Sponsor, believed that the ELC framework, including testing, only applied to development projects and did not pertain to infrastructure projects following the commercial off-the-shelf path methodology. However, we believe that the ELC framework is applicable, and we have issued prior reports[16] recommending that development projects, including infrastructure projects as well as projects that implement a commercial off-the-shelf solution, need to follow the ELC framework. In each of these reports, IT organization management agreed with our recommendations concerning adherence to the ELC framework.

In November 2019, Internal Revenue Manual 2.16.1 was updated to remove all references to infrastructure projects and clarified that all ELC projects are either new development projects or maintenance projects. There are no longer any infrastructure projects. Subsequent to our report on e-mail records management, in September 2020 the Strategy and Planning function's Director, Business Planning and Risk Management, issued interim guidance that will eventually update Internal Revenue Manual 2.16.1, clarifying that all ELC projects must follow the development phases, including testing. Inadequate testing substantially increases the risk that the system will not perform as intended or will cause undesirable effects to other interfacing systems when placed into production.

The Chief Information Officer should ensure that:

Recommendation 3: The *Simplified Design Specification Report* for network segmentation is updated to describe the complexity of the design and the limits of the Identity Services Engine and TrustSec products.

Management's Response: The IRS disagreed with this recommendation. Updates to the design and complexities of the Identity Services Engine and TrustSec belong in the Unified Segmentation Audit Operations artifact.

Office of Audit Comment: The IRS states that updates concerning the Identity Services Engine and TrustSec products belong in the Unified Segmentation Audit Operations artifact rather than the *Simplified Design Specification Report*; however, the IRS did not state that the artifact would be updated. The IRS needs to ensure that the Unified Segmentation Audit Operations artifact is updated to describe the complexity of the design and the limits of the Identity Services Engine and TrustSec products.

[16] Treasury Inspector General for Tax Administration, Report No. 2015-20-073, *Inadequate Early Oversight Led to Windows Upgrade Project Delays* (Sept. 2015); Treasury Inspector General for Tax Administration, Report No. 2019-20-060, *E-Mail Records Management Is Generally in Compliance With the Managing Government Records Directive* (Sept. 2019); and Treasury Inspector General for Tax Administration, Report No. 2021-20-066, *The Data at Rest Encryption Program Has Made Progress With Identifying Encryption Solutions, but Project Management Needs Improvement* (Sept. 2021).

Recommendation 4: A *System Test Plan* is developed and executed for network segmentation to include test cases for key requirements, test results, and test case resolution for failed tests.

Management's Response: The IRS agreed with this recommendation. The IRS will revise the *System Test Plan* with updates on the additional specific test case requirements, test results, and test case resolution on failed tests.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to evaluate the effectiveness of IT organization efforts to limit the internal network risk exposure by segmenting key information technology systems. To accomplish our objective, we:

- Reviewed the responsibilities of the UNS Governance Board and the UNS Governance Board meeting minutes to evaluate the effectiveness of information technology governance over the SEG Project.
- Reviewed the ELC framework and related ELC documents to evaluate the SEG Project's compliance with development processes.
- Reviewed Cisco's Identity Services Engine and TrustSec product documentation and attended a demonstration with UNS function personnel who explained how the products are used in the design of network segmentation for the IMF.
- Obtained audit log data for December 1, 2020, after network segmentation had been deployed for the IMF. We received audit logs showing 1,441 audit log records and selected a judgmental sample[1] of 30 of the 75 users who had accessed IMF resources during a four-hour period to determine whether management had properly authorized their access to the IMF resources. We selected a judgmental sample because we did not plan to project the results to the population.
- Reviewed configuration settings and the results of Identity Services Engine and TrustSec queries to validate that the classification, propagation, and enforcement phases of network segmentation were enabled.
- Reviewed the Identity Services Engine authorization rules to verify network segmentation was enabled to deploy access controls for the IMF.
- Reviewed the authorization policies to determine whether the authorization rules were reasonable and complete.

Performance of This Review

This review was performed with information obtained from the IT organization's UNS function located in New Carrollton, Maryland, during the period November 2020 through September 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.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

Major contributors to the report were Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Bryce Kisler, Director; Carol Taylor, Audit Manager; Denis Danilin, Lead Auditor; and William Varnadore, Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of the data from the audit log file. We evaluated the data by: 1) visually reviewing the output file to detect missing data; 2) verifying the number of records in the raw input file and output file were the same to ensure the completeness of the output file; and 3) communicating with IRS officials knowledgeable about the data to obtain a count of the total number of log records. We determined that the data were sufficiently reliable for the purposes of this report.

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: the configuration, policies, rules, and audit logs of Cisco's Identity Services Engine and TrustSec products; the ELC framework; the IT organization's governance process; the information technology security, policy, and guidance requirements; and the information technology testing standards.

We evaluated these controls by reviewing the criteria applicable to network segmentation, assessing the SEG Project's governance process, interviewing UNS and Cybersecurity function personnel, and reviewing SEG Project documentation. We verified that the IMF network segmentation was effective by analyzing the Identity Services Engine and TrustSec products' configuration, authorization policies, and related rules. In addition, we evaluated audit log activities to verify that network segmentation was effective. We also analyzed a judgmental sample of users from the audit log who accessed the IMF resources and confirmed that the users were properly authorized through the Online 5081 process.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

January 12, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Chief Information Officer

Nancy A. Sieger
Digitally signed by Nancy A. Sieger
Date: 2022.01.12 10:38:18 -05'00'

SUBJECT: Draft Audit Report – Network Segmentation Reduced Unnecessary Access to Individual Master File Resources; However, Governance and Development Processes Were Not Always Followed (Audit #202120014)

Thank you for the opportunity to review the draft audit report and to discuss the report's observations with the Network Segmentation project team. We are committed to protecting the IRS networks, assets, and taxpayer data from unauthorized users and devices.

Network Segmentation is an important enterprise solution with the goal to increase cybersecurity operations and safeguard against cyber-attacks. Network Segmentation represents an initiative we have emplaced to strengthen network security. Effectively, in protecting the High Value Assets, the IRS' Individual Master File (IMF) Network Segmentation was completed ahead of schedule, within budget and with project development artifacts on archive.

Prior to the issuance of the report, our IT leadership shared concerns about the audit findings with the TIGTA audit team on areas of project governance and development processes. Recommendations 2 and 3 align with those processes. While we acknowledge the importance of these areas, we disagree with TIGTA's findings and conclusions related to deficiencies in the project's governance and documentation.

Network Segmentation was approved prior to production deployment by our IT leadership and IT senior executive leadership as governing sponsors. The approved project development artifacts were also completed in accordance with the guidelines of our project management practices. Additional information was provided to the TIGTA audit team; however, it appears we did not reach consensus on the interpretation on project governance and approvals.

Attached is our Corrective Action Plan to address the audit recommendations.
We are committed to strengthening project management practices while maintaining agility to meet Cybersecurity directives and the mission of the IRS.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Frank Kist Director, Network Engineering at (240) 613-4041.

Attachment

Attachment

Draft Audit Report – Network Segmentation (Audit #202120014)

RECOMMENDATION 1: ELC framework artifacts are completed and Milestone Exit Reviews are conducted by network segmentation projects, prior to deployment to production.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. We will complete the required ELC artifacts for future Network Segmentation efforts, deemed as a project, prior to deployment into production.

IMPLEMENTATION DATE: August 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress monthly until completion.

RECOMMENDATION 2: Project teams obtain governance board approvals prior to deploying development project solutions to production.

CORRECTIVE ACTION #2: The IRS disagrees with this recommendation. Governance Process is established and followed for delivering project solutions – however, Senior leadership approval may often come prior to governance approval, Governance and Artifacts are then updated and finalized.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the JAMES and review remediation progress monthly until completion.

RECOMMENDATION 3: The Simplified Design Specification Report for network segmentation is updated to describe the complexity of the design and the limits of the Identity Services Engine and TrustSec products.

CORRECTIVE ACTION #3: The IRS disagrees that the SDSR needs further description of the complexity of the design and limits of the ISE and TrustSec products. Updates to the design and complexities of ISE and TrustSec belong in the Unified Segmentation Audit Operations artifact.

IMPLEMENTATION DATE: N/A

Attachment

Draft Audit Report – Network Segmentation (Audit #202120014)

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the JAMES and review remediation progress monthly until completion.

RECOMMENDATION 4: A System Test Plan is developed and executed for Network Segmentation to include test cases for key requirements, test results, and test case resolution for failed tests.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. We will revise the System Test Plan with updates on the additional specific test case requirements, test results, and test case resolution on failed tests.

IMPLEMENTATION DATE: August 15, 2022

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, User & Network Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the JAMES and review remediation progress monthly until completion.

Appendix III

Glossary of Terms

Term	Definition
Acceptance Testing	Testing that verifies if the installed code or software works as intended.
[redacted]	[redacted]
Administration Node	A Cisco Identity Services Engine node used to perform all administrative operations.
Artifact	The tangible output of an activity performed by a project during its development life cycle.
[redacted]	[redacted]
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Authorization Policy	A policy composed of authorization rules, including the element's name, attributes, and permissions.
Commercial Off-the-Shelf	Prepackaged, vendor-supplied software that will be used with little or no modification to provide all or part of a development solution.
Common Communication Gateway	A portion of the IRS network that provides Internet connectivity and external data connectivity to Federal, State, and local government agencies and tax partners.
Core Switch	A high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network or the Internet, and provide the final aggregation point for the network.
[redacted]	[redacted]
Enterprise Computing Center	IRS facilities that support tax processing and information management through a data processing and telecommunications infrastructure.
Enterprise Remote Access Program	The IRS program responsible for managing virtual private network access to the internal network.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.

Term	Definition
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers and is usually internal to an organization and deployed within owned facilities.
Internet Protocol Address	A unique number assigned to every computer or device that is connected to the Internet.
Local Area Network	A group of computers and associated devices that share a common communications line or wireless link to a server. It typically encompasses computers and peripherals connected to a server within a distinct geographic area such as an office or a commercial establishment. Computers and other mobile devices use the connection to share resources, such as printer or network storage.
Logical Partition	A subset of a single physical computer system that contains resources (processors, memory, and input/output devices), and which operates as an independent system.
Network Access Device	Entry points for users and devices into the network.
Online 5081	An IRS web-based application that allows users to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems.
Packet	In networking, a packet is a small segment of a larger message. Data sent over computer networks, such as the Internet, are divided into packets. The computer or device that receives them then recombines these packets.
Penetration Testing	Testing in which assessors, using all available documentation (*e.g.*, system design, source code, and system manuals) and working under specific constraints, attempt to circumvent the security features of a system.
Policy Service Node	A Cisco Identity Services Engine node with the policy service persona that evaluates policies and makes all decisions related to network access and other services.
Privacy Testing	Testing that verifies that the system meets the privacy requirements.
Production	The computing environment where the approved production programs that run an organization are executed; this includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Project Tailoring Plan	A documented agreement between the project manager, organization, and process owner(s) regarding how the project will meet the established process requirements. This document identifies the process artifacts and reviews required to be completed by the project and any provisions or exceptions to the processes.
Propagation	The means by which a Security Group Tag is carried between networking devices.
Resource Access Control Facility	An IBM software product that provides basic security for a mainframe system and protects resources by granting access only to authorized users.

Term	Definition
Router	A device or, in some cases, software on a computer that determines the best way for a packet to be forwarded to its destination.
Security Group Access Control List	A list that restricts or permits access to specific resources.
Security Testing	A process to determine that an information system protects data and maintains functionality as intended.
Switch	Connects multiple devices, such as computers, printers, and servers. A switch enables connected devices to share information and communicate with each other.
System Integration Testing	Testing that is conducted to verify that the system is integrated properly and functions as intended.
Virtual Private Network	A restricted-use computer network that is constructed from the system resources of a network.
Wide Area Network	A network that spans a large geographic area such as a city, State, or country.
Wired	A connection method that connects to the local area network using physical cables and circuits at a specific location.
Wireless	A connection method that connects to the local area network without physically connecting the device through a wired connection.

Appendix IV

Abbreviations

ELC	Enterprise Life Cycle
HVA	High Value Asset
IBM	International Business Machines
IMF	Individual Master File
IRS	Internal Revenue Service
IT	Information Technology
SEG	Network Segmentation
UNS	User and Network Services

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.